PŘIHLÁŠKA VYNÁLEZU

Zveřejněná podle §31 zákona č. 527/1990 Sb.

(21) Číslo dokumentu:

2015-472

(13) Druh dokumentu: **A3**

(51) Int. Cl.:

G06Q 30/02	(2012.01)
G06F 21/30	(2013.01)
G06F 21/31	(2013.01)
G06F 21/44	(2013.01)
H04L 29/02	(2006.01)

(19) ČESKÁ REPUBLIKA

ÚŘAD PRŮMYSLOVÉHO VLASTNICTVÍ

(22) Přihlášeno: **07.07.2015**

(40) Datum zveřejnění přihlášky vynálezu: **08.02.2017**
(Věstník č. 6/2017)

(71) Přihlašovatel:
ADUCID s.r.o., Brno - Přízřenice, CZ

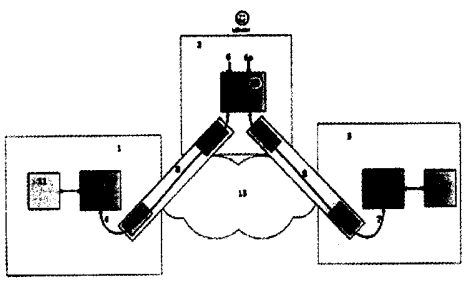
(72) Původce:
Ing. Libor Neumann, CSc., Praha 5 - Lužiny, CZ

(74) Zástupce:
INVENTIA s. r. o., RNDr. Kateřina Hartvichová, Na Bělidle 3, 150 00 Praha 5

(54) Název přihlášky vynálezu:

Způsob navazování chráněné elektronické komunikace, bezpečného přenášení a zpracování informací mezi třemi a více subjekty

(57) Anotace:
Předkládané řešení poskytuje způsob navazování chráněné elektronické komunikace, bezpečného přenášení a zpracování informací mezi třemi a popřípadě více subjekty v němž se nejprve s pomocí autentizačního systému vytvoří první bezpečný autentizovaný kanál mezi prvním subjektem a druhým subjektem, prostřednictvím kterého první subjekt ve spolupráci s druhým subjektem vytvoří autentizační objekt uložený na druhém subjektu a vybavený metodami autentizačního objektu, přičemž metody autentizačního objektu nastaví první subjekt tak, že ke každé metodě autentizačního objektu přiřadí informaci o právech alespoň jednoho dalšího subjektu, a popřípadě i prvního subjektu, používat alespoň jednu metodu autentizačního objektu, a první bezpečný autentizovaný kanál se uzavře.



CZ 2015 - 472 A3

Způsob navazování chráněné elektronické komunikace, bezpečného přenášení a zpracování informací mezi třemi a více subjekty

Oblast techniky

Vynález se týká způsobu navazování chráněné elektronické komunikace mezi třemi a více subjekty současně včetně bezpečné identifikace a ověření identity subjektů při elektronické komunikaci a také bezpečného provádění přenosu a zpracování informací při elektronické komunikaci mezi třemi a více subjekty a to jak pro vzdálenou tak lokální elektronickou komunikaci a jejich kombinace.

Dosavadní stav techniky

U většiny známých způsobů chráněné elektronické komunikace se jedná o komunikaci dvou subjektů, poskytovatele služby a uživatele služby. Navazování chráněné elektronické komunikace je přitom přímo spojeno s cílovým systémem, se kterým je elektronická komunikace navazována.

V současné době nejrozšířenějším způsobem navazování chráněné elektronické komunikace je použití přihlašovacího jména a hesla (loginname/password).

Existují také další způsoby navazování chráněné elektronické komunikace, kde je do navazování chráněné elektronické komunikace začleněno více typů subjektů. Jedná se například o systémy Public Key Infrastructure (PKI), kde kromě uživatele (User) a poskytovatele služby (Relying party) existuje ještě certifikační autorita (Certification Authority) případně také registrační autorita (Registration Authority). Certifikační autorita a případně registrační autorita jsou začleněny do procesu přípravy prostředí chráněné elektronické komunikace tím, že ověřují identitu uživatele a vydávají a elektronicky podepisují certifikát, který je potom následně používán poskytovatelem služby a uživatelem služby k navázání jejich chráněné elektronické komunikace.

Jiný dnes stále častěji používaný způsob navazování chráněné elektronické komunikace je založen na principu Federativní identity. Jedná se např. standardy SAML, oAuth, OpenId, WS-federation. Zde je dalším subjektem zapojeným do navazování chráněné elektronické komunikace poskytovatel identity (Identity Provider). Základní způsob principu Federativní identity je, že uživatel služby při přístupu na systém poskytovatele služby je přesměrován na

systém poskytovatele identity, kde je provedena autentizace uživatele a po ukončení autentizace je uživatel přesměrován zpět na systém poskytovatele služby. Přitom poskytovatel identity předá poskytovateli služby informace o výsledku autentizace uživatele. K přesměrování uživatele mezi poskytovatelem služby a poskytovatelem identity a zpět je používána speciální funkčnost HTTP protokolu vestavěná ve standardních webových prohlížečích (HTTP redirect). Uživatel je přesměrován jen k provedení autentizace. Přenos a zpracování cílových informací pobíhá mezi dvěma subjekty, mezi poskytovatelem služby a uživatelem.

Existují ještě další způsoby navazování chráněné elektronické komunikace, některé založené na existenci různých jedinečných hardwarových tokenů, multikanálové způsoby, které k navazování chráněné komunikace využívají různé, navzájem více či méně nezávislé komunikační kanály, ale také nové vysoce automatizované způsoby navazování chráněné elektronické komunikace, popsané např. v patent. přihlášce PV 2013-373 - Způsob autentizace bezpečného datového kanálu.

Po tom, co je některým z výše uvedených způsobů, nebo jiných způsobů (dále označovaných jako autentizační systémy), navázána chráněná elektronická komunikace mezi dvěma subjekty, a dojde tak k zabezpečení komunikačního kanálu, přenášejí tyto dva subjekty informace chráněným způsobem, případně tyto informace dále chráněným způsobem zpracovávají.

Vedle toho však existují specializované systémy nebo aplikace, které umožňují komunikaci více subjektů navzájem, jako jsou telekonference, systémy sociálních sítí, ale také elektronické platby, elektronické vstupenky, elektronické jízdenky, apod. Některé z takových systémů vyžadují také chráněnou elektronickou komunikaci, výměnu a zpracování informací, kde je bezpečně zajištěno, že mezi sebou komunikují právě identifikovatelné subjekty a ne nikdo jiný a že komunikace je chráněna ve všech složkách bezpečnosti (integrita, důvěrnost, dostupnost a nepopiratelnost).

V případě, že tyto systémy vyžadují chráněnou komunikaci, užívají některých známých způsobů navazování chráněné elektronické komunikace mezi dvěma subjekty. Tedy vždy pro každého uživatele a každého poskytovatele odděleně. To způsobuje určité komplikace.

V realitě dochází k tomu, že buď jsou systémy navazování komunikace mezi více subjekty přijatelně jednoduché pro uživatele, ale zároveň nezajišťují potřebnou bezpečnost (např. opakované vyžadování zadávání hesel) nebo potřebnou bezpečnost zajistit mohou, ale jsou

uživatelsky natolik komplikované, že je většina uživatelů v reálné praxi nezvládá (např. PKI) a odmítá je používat.

Přitom v praxi existuje celá řada situací, kde spolu potřebuje komunikovat více subjektů současně. Zároveň jde o situace, kdy je nutné zajistit vysokou úroveň ochrany, ale které by měla zvládat většina uživatelů. Jedná se například o elektronické jízdné v hromadné dopravě různého typu, potvrzování a ověřování identity v obchodě a bankovnictví jako jsou internetové platby, transakce ve veřejné správě včetně přeshraniční komunikace, komunikace ve zdravotnictví, apod.

Podstata vynálezu

Předmětem vynálezu je způsob navazování chráněné elektronické komunikace, bezpečného přenášení a zpracování informací mezi třemi a více subjekty vyznačující se tím, že všechny subjekty jsou vybaveny autentizačním systémem a tím, že se nejprve vytvoří a zkonfiguruje pro daný účel specifický objekt (dále jen autentizační objekt), který se pak následně využije určitým způsobem nebo kombinací určitých způsobů pro navazování chráněné elektronické komunikace, přenášení a zpracování informací mezi těmito subjekty.

Založení a konfigurace autentizačního objektu

Nejprve s pomocí autentizačního systému vytvoří první bezpečný autentizovaný kanál mezi prvním subjektem (server) a druhým subjektem (zařízení uživatele), prostřednictvím kterého první subjekt ve spolupráci s druhým subjektem vytvoří autentizační objekt uložený na druhém subjektu a vybavený metodami autentizačního objektu, přičemž metody autentizačního objektu nastaví první subjekt tak, že ke každé metodě autentizačního objektu přiřadí informaci o právech alespoň jednoho dalšího subjektu, a popřípadě i prvního subjektu, používat alespoň jednu metodu autentizačního objektu, a první bezpečný autentizovaný kanál se uzavře.

Autentizační objekt může s výhodou obsahovat interní data pro budoucí použití (např. podpisové kryptografické klíče, osobní údaje, biometrická data, údaje o předplaceném jízdném nebo jiných službách.

Práva používat příslušné metody autentizačního objektu nastavuje první subjekt, který autentizační objekt vytvořil a zkonfiguroval tak, že ke každé metodě autentizačního objektu

přiřadí, který subjekt, případně skupina subjektů, může či nesmí jednotlivou metodu autentizačního objektu používat.

První subjektem je server, s nímž ostatní subjekty komunikují, může to být například server poskytovatele služeb

Druhým subjektem je elektronické zařízení, které používá uživatel. Může jím být například počítač, mobilní telefon, tablet, chytré hodinky, apod. Toto zařízení zajišťuje s vysokou bezpečností jistotu, že neexistuje jiné podobné zařízení nerozpoznatelné elektronickými prostředky od zařízení uživatele; podporuje způsob vytváření či propojování dalších zařízení téhož uživatele bezpečným způsobem, přičemž zaručují odlišitelnost jednotlivých zařízení elektronickými prostředky.

Metoda autentizačního objektu je předem nastavené chování autentizačního objektu, které se mění v závislosti na vstupních parametrech použitých při spuštění této metody.

Chráněná současná elektronická komunikace mezi třemi nebo více subjekty

S pomocí autentizačního systému se vytvoří první bezpečný autentizovaný kanál mezi druhým subjektem a třetím subjektem (další server), pomocí kterého se aktivuje metoda autentizačního objektu, která iniciuje s pomocí autentizačního systému vytvoření druhého bezpečného autentizovaného kanálu mezi druhým subjektem a prvním subjektem nebo jiným subjektem, přičemž druhý bezpečný autentizovaný kanál existuje současně s prvním bezpečným autentizovaným kanálem a využijí se k následnému zabezpečenému přenášení informací mezi všemi subjekty.

Metoda autentizačního objektu může vytvořit s pomocí autentizačního systému dva nebo více bezpečných autentizovaných kanálů mezi druhým subjektem a dvěma nebo více dalšími subjekty, které existují současně s prvním bezpečným autentizovaným kanálem, a všechny takové bezpečné autentizované kanály se společně využijí k následnému zabezpečenému přenášení informací mezi všemi subjekty.

Třetí subjekt je server, s nímž ostatní subjekty komunikují, různý od prvního subjektu.

Chráněná komunikace mezi dvěma subjekty přes třetí subjekt navázaná při využití lokální komunikace

První subjekt vytvoří nezávisle na sobě autentizační objekty vybavené metodami těchto autentizačních objektů druhému subjektu a čtvrtému subjektu, přičemž druhý subjekt a první subjekt mezi sebou následně s pomocí autentizačního systému vytvoří první bezpečný

autentizovaný kanál, pomocí kterého se aktivuje metoda autentizačního objektu druhého subjektu, která připraví ve spolupráci s prvním subjektem identifikační informace určené k propojení druhého subjektu se čtvrtým subjektem a také bezpečnostní informace určené k následnému zabezpečení komunikace mezi druhým subjektem a čtvrtým subjektem, přičemž identifikační informace a bezpečnostní informace, které jsou známy pouze druhému subjektu, se z druhého subjektu přenesou na čtvrtý subjekt a následně se mezi prvním subjektem a čtvrtým subjektem s pomocí autentizačního systému vytvoří druhý bezpečný autentizovaný kanál, který se pomocí identifikačních informací propojí s prvním bezpečným autentizovaným kanálem, čímž se bezpečnostní informace stanou dostupné prvnímu subjektu a použijí se k následnému zabezpečenému přenášení informací mezi druhým subjektem a čtvrtým subjektem prostřednictvím prvního subjektu.

Identifikační informace a bezpečnostní informace se mohou s výhodou přenášet z druhého subjektu na čtvrtý subjekt pomocí lokální komunikace.

Čtvrtý subjekt je jiné zařízení stejného či jiného uživatele.

Lokální komunikace je komunikace na malou vzdálenost, která vylučuje, že komunikující subjekty sdělí informaci třetí osobě nebo že tato komunikace bude odposlechnuta.

Identifikační informace jsou informace, pomocí kterých lze v rámci jednoho subjektu propojit jeden bezpečný autentizovaný kanál s jedním či více dalších bezpečných autentizovaných kanálů tak, že subjekty propojené těmito bezpečnými autentizovanými kanály mohou komunikovat mezi sebou.

Bezpečnostní informace jsou informace sloužící k navázání chráněné elektronické komunikaci mezi dvěma komunikujícími subjekty.

Spuštění metody autentizačního objektu konstantní lokální komunikací

V jednom výhodném provedení se při vytvoření a konfiguraci autentizačního objektu a jeho metod podle způsobu "Založení a konfigurace autentizačního objektu" v rámci interních dat pro budoucí použití autentizačního objektu na druhém subjektu nastaví spouštěcí informace pro lokální spuštění metody autentizačního objektu, která se následně spustí samotným druhým subjektem nebo pomocí lokální komunikace s dalším zařízením obsahujícím sejmutou informaci, která spouštěcí informaci odpovídá předem zvoleným způsobem, přičemž po svém spuštění metoda autentizačního objektu s využitím interních dat pro budoucí použití a s pomocí autentizačního systému vytvoří jeden nebo více autentizovaných kanálů,

které se použijí k následnému zabezpečenému přenášení informací mezi druhým subjektem a jedním nebo více dalších subjektů dle konfigurace autentizačního objektu.

Informace pro spuštění metody autentizačního objektu může být s výhodou doplněna o informace získané během lokální komunikace při spouštění metody.

Skládání

Pro dosažení požadované funkčnosti v příslušném specifickém použití vynálezu je zejména výhodné kombinovat některá nebo všechna zde popsaná výhodná provedení dohromady.

Například pro zajištění topologie typu dva poskytovatelé služeb, jeden uživatel je možné využít *Chráněná současná komunikace mezi třemi nebo více subjekty.*

Například pro zajištění topologie typu jeden poskytovatel služeb, dva uživatelé je možné využít *Chráněná komunikace mezi dvěma subjekty přes třetí subjekt navázaná při využití lokální komunikace.*

Například pro zajištění topologie typu dva poskytovatelé, dva uživatelé je možné použít *Chráněná současná komunikace mezi třemi nebo více subjekty* a také *Chráněná komunikace mezi dvěma subjekty přes třetí subjekt navázaná při využití lokální komunikace.*

Například pro zajištění topologie typu jeden poskytovatel služeb, jeden uživatel, jedna věc nebo jedno zařízení je možné využít *Spuštění metody autentizačního objektu konstantní lokální komunikací.*

Přehled obrázků na výkresech

Obr.1 – Schematické zobrazení způsobu Založení a konfigurace autentizačního objektu podle příkladu provedení vynálezu č. 1, 2, 3, 4, 5, 6, 7, 8, 9.

Obr.2 – Schematické zobrazení způsobu Současná komunikace mezi třemi nebo více subjekty podle příkladu provedení vynálezu č. 1, 6, 8.

Obr.3 – Schematické zobrazení způsobu Chráněná komunikace mezi dvěma subjekty přes třetí subjekt navázaná při využití lokální komunikace podle příkladu provedení vynálezu č. 2.

Obr.4 – Schematické zobrazení způsobu Spuštění personálního objektu konstantní lokální komunikací podle příkladu provedení vynálezu č. 5, 7.

Obr.5 – Schematické zobrazení kombinace způsobů Současná komunikace mezi třemi nebo více subjekty a Lokální propojení dvou klientských systémů při komunikaci tří subjektů podle příkladu provedení vynálezu č. 4.

Obr.6 – Chráněná komunikace mezi dvěma subjekty přes třetí subjekt navázaná při využití lokální komunikace podle příkladu provedení vynálezu č. 9.

Obr.7 – Schematické zobrazení způsobu Chráněná komunikace mezi dvěma subjekty přes třetí subjekt navázaná při využití lokální komunikace podle příkladu provedení vynálezu č. 3.

Obr.8 – Schematické zobrazení způsobu Chráněná komunikace mezi dvěma subjekty přes třetí subjekt navázaná při využití lokální komunikace podle příkladu provedení vynálezu č. 3.

Obr.9 – Schematické zobrazení způsobu Spuštění personálního objektu konstantní lokální komunikací podle příkladu provedení vynálezu č. 2.

Příklady provedení vynálezu

Příklad 1 - Způsob provedení platby mezi třemi subjekty

Využívá způsob "Založení a konfigurace autentizačního objektu" a způsob "Chráněná současná komunikace mezi třemi nebo více subjekty".

Dle Obr. 1.

Druhý subjekt 2 ("uživatel") spolu s Prvním subjektem 1 ("banka") vytvoří pomocí Autentizačního systému 8, který má Serverovou část 8a Autentizačního systému 8 a Klientskou část 8b Autentizačního systému 8, První bezpečný autentizovaný kanál 4 mezi Prvním subjektem 1 a Druhým subjektem 2. První subjekt 1 vytvoří s využitím Prvního bezpečného autentizovaného kanálu 4 nový Autentizační objekt 5 ("platební modul") na zařízení Druhého subjektu 2. U tohoto Autentizačního objektu 5 nastaví pravidla řízení přístupu k Metodám 6 Autentizačního objektu 5 tak, že umožní použití Metody 6a ("zaplať") Autentizačního objektu 5 pro další subjekt nebo subjekty ("prodejce"). Dále První subjekt 1 může pomocí Metody 6b ("vytvoř kryptomateriál") Autentizačního objektu 5 vyžádat vytvoření kryptografického materiálu, který je uložen jako součást interních dat X5 pro budoucí použití Autentizačním objektem 5 pro účely potvrzování platebních transakcí. První bezpečný komunikační kanál 4 mezi Prvním subjektem 1 a Druhým subjektem 2 se uzavře.

Dle Obr. 2.

V době kdy Druhý subjekt 2 komunikuje vzdáleně s Třetím subjektem 3 ("prodejce") a chce provést platbu se vytvoří Druhý bezpečný autentizovaný kanál 7 pomocí Autentizačního

systému 8, který má Serverovou část 8a Autentizačního systému 8 a Klientskou část 8b Autentizačního systému 8, použitého mezi Druhým subjektem 2 a Třetím subjektem 3 a s využitím tohoto Druhého bezpečného autentizovaného kanálu 7 vyžádá Třetí subjekt 3 provedení Metody 6a Autentizačního objektu 5 včetně předání příslušných parametrů platby jako je placená částka, účet prodejce atd.

Požadavek provedení platby ve formě požadavku na provedení Metody 6a Autentizačního objektu 5 a parametry platby jsou přeneseny například z Informačního systému 12 Třetímu subjektu 3 do Rozhraní 10 Autentizačních objektů 5 Třetího subjektu 3 a dále vytvořeným Druhým bezpečným autentizovaným kanálem 7 mezi Třetím subjektem 3 a Druhým subjektem 2.

Druhý subjekt 2 vyhodnotí nastavená přístupová pravidla Metody 6a Autentizačního objektu 5 pro konkrétní Třetí subjekt 3 a v případě shody pokračuje ve zpracování. V případě neshody zpracování požadavku na platbu odmítne.

Pokud zpracování pokračuje, vytvoří Metoda 6a Autentizačního objektu 5 s pomocí Autentizačního systému 8 První bezpečný autentizovaný kanál 4 mezi Druhým subjektem 2 a Prvním subjektem 1, který existuje současně s Druhým bezpečným autentizovaným kanálem 7 mezi Druhým subjektem 2 a Třetím subjektem 3. Pomocí Prvního bezpečného autentizovaného kanálu 4 a Rozhraní 9 Autentizačních objektů 5 Prvního subjektu 1 jsou přenášeny zprávy mezi Autentizačním objektem 5 a Informačním systémem 11 Prvního subjektu 1 potřebné k zadání a potvrzení platby včetně potřebného potvrzování uživatelem a kryptografických operací pomocí dříve vytvořeného kryptografického materiálu. Po úspěšném provedení platby či po jejím odmítnutí Prvním subjektem 1 či Druhým subjektem 2 je výsledek a případně další informace přenesen pomocí Druhého bezpečného autentizovaného kanálu 7 mezi Druhým subjektem 2 a Třetím subjektem 3 například do Informačního systému 12 Třetího subjektu 3 jako návratová zpráva požadavku provedení platby.

Dle Obr. 1.

V průběhu času může První subjekt 1 používat další Metody 6 Autentizačního objektu 5 sloužící k údržbě platebního Autentizačního objektu 5 jako je vytvoření nového kryptografického materiálu včetně potvrzení následnosti známými kryptografickými metodami. Při tom může využívat Rozhraní 9 Autentizačních objektů 5 Prvního subjektu 1, První bezpečný autentizovaný kanál 4 vytvořený Autentizačním systémem 8, Metody 6

Autentizačního objektu 5 na zařízení Druhého subjektu 2 a pravidla řízení přístupu k Metodám 6 Autentizačního objektu 5.

Komunikace mezi subjekty probíhá pomocí Obecné sítě 13, která nemusí být zabezpečena, např. pomocí Internetu.

Příklad 2 - Anonymní jízdní doklady

Využívá způsob "Založení a konfigurace autentizačního objektu" a způsob "Spuštění metody autentizačního objektu konstantní lokální komunikací".

Dle Obr. 2.

Druhý subjekt 2 ("cestující") zakoupí u Třetího subjektu 3 ("dopravce") digitální anonymní jízdenku např. postupem podle příkladu 1. Výsledkem nákupu jízdenky je Autentizační objekt 5 ("jízdenka") Druhého subjektu 2 ("cestující") a případně další interní data X5 pro budoucí použití např. identifikace jízdenky, tarif, cena, platnost atd. v Informačním systému 12 Třetího subjektu 3 ("dopravce").

Informační systém 12 Třetího subjektu 3 ("dopravce") nastaví také přístupová práva k Metodám 6 Autentizačního objektu 5 ("jízdenka") Druhého subjektu 2 ("cestující") dle svých potřeb a v souladu s právními předpisy a také způsoby spouštění Metod 6 Autentizačního objektu 5 ("jízdenka") pomocí Lokální komunikace 16. (obr. 3, obr. 4).

Dle Obr. 9.

V případě vstupní kontroly Dalším subjektem 20 např. pomocí zařízení typu vstupní brána dopravního prostředku (např. turniket) je Lokální komunikací 16 předána Sejmutá informace X4 mezi Dalším subjektem 20 a Druhým subjektem 2 např. zobrazením QR kódu vstupní branou a sejmutím QR kódu pomocí zařízení Druhého subjektu 2. V případě, že Sejmutá informace X4 odpovídá Spouštěcí informaci X3 aktivuje se ověřovací Metoda 6 ("zkontroluj jízdné pomocí statického identifikátoru vstupní brány") Autentizačního objektu 5.

Metoda 6 ("zkontroluj jízdné pomocí statického identifikátoru vstupní brány") Autentizačního objektu 5 ("jízdenka") vytvoří Druhý bezpečný autentizovaný kanál 7 pomocí Autentizačního systému 8 použitého mezi Druhým subjektem 2 a Třetím subjektem 3 a pomocí tohoto Druhého bezpečného autentizovaného kanálu 7 a Rozhraní 10 Autentizačních objektů 5 Třetího subjektu 3 provede Metoda 6 ("zkontroluj jízdné pomocí vstupní brány")

Autentizačního objektu 5 ("jízdenka") Druhého subjektu 2 ("cestující") ve spolupráci s Informačním systémem 12 Třetího subjektu 3 ("dopravce") verifikaci jízdného. Dle Obr. 3.
V případě kontroly jízdného Čtvrtým subjektem 14 ("revizor") Druhý subjekt 2 ("cestující") pomocí zařízení Druhého subjektu 2 a Lokální komunikace 16 mezi zařízením Druhého subjektu 2 ("cestující") a zařízením Čtvrtého subjektu 14 ("revizor") předá identifikační informaci X1 pomocí Metody 6 ("kontrola jízdného revizorem") Autentizačního objektu 5 ("jízdenka"), např. tím, že zařízení Druhého subjektu 2 ("cestující") zobrazí QR kód obsahující unikátní číslo jízdenky. Zařízení Druhého subjektu 2 ("cestující") je vůči zařízení Čtvrtého subjektu 14 ("revizor") použito způsobem jako by šlo o Další subjekt 20. (dle Obr. 4).

Dle Obr. 3.
Čtvrtý subjekt 14 ("revizor") pomocí zařízení Čtvrtého subjektu 14, ve kterém je Autentizačním objekt 5 ("kontrola") Čtvrtého subjektu 14 zřízený předtím Třetím subjektem 3 ("dopravce") (např. který byl zřízen Informačním systémem 12 Třetího subjektu 3 ("dopravce") dříve v procesu vzniku smluvního vztahu mezi dopravcem a revizorem např. jako součást zaškolení a ověření znalostí zaměstnance) přečte Sejmutou informaci X4 ze zařízení Druhého subjektu 2 ("cestující") a pomocí Metody 6 Autentizačního objektu 5 ("zkontroluj jízdné revizorem") Čtvrtého subjektu 14 předá informace k ověření do Informačního systému 12 Třetího subjektu 3 ("dopravce"). K tomu využije Třetího bezpečného autentizovaného kanálu 15 vytvořeného pomocí Autentizačního systému 8 a Rozhraní 10 Autentizačních objektů 5 Třetího subjektu 3. Poté od Informačního systému 12 Třetího subjektu 3 ("dopravce") dostane pomocí Třetího bezpečného autentizovaného kanálu 15 výsledek ověření a případně další potřebné informace.

Příklad 3 - Personifikované cestovní doklady.

Využívá způsob "Založení a konfigurace autentizačního objektu" a způsob "Chráněná komunikace mezi dvěma subjekty přes třetí subjekt navázaná při využití lokální komunikace".

Dle Obr. 2.
Druhý subjekt 2 ("cestující") zakoupí u Třetího subjektu 3 ("dopravce") digitální jízdenku, která je nepřenosná. Při tom jsou užity osobní údaje například fotografie či jiná biometrická

data, které dopravce nesmí ze zákonných či jiných důvodů uchovávat nebo je nechce uchovávat v žádném svém informačním systému, tedy ani v Informačním systému 12 Třetího subjektu 3 ("dopravce"). Koupě může proběhnout podle příkladu 1 s případným začleněním postupu ověření osobních údajů.

Výsledkem je elektronická jízdenka uschovaná v Autentizačním objektu 5 ("jízdenka") Druhého subjektu 2 ("cestující") a v Informačním systému 12 Třetího subjektu 3 ("dopravce") a další připojená interní data X5 pro budoucí použití např. tarif, cena, platnost atd. a také osobní údaje sloužící k identifikaci uživatele při kontrole cestovních dokladů, např. biometrická data jako fotografie, která jsou uložena pouze v Autentizačním objektu 5 ("jízdenka") Druhého subjektu 2 ("cestující"), a která mohou být kryptograficky zajištěna proti modifikaci např. elektronickým podpisem Třetího subjektu 3 ("dopravce").

Dle Obr. 3.

V případě kontroly jízdného Čtvrtým subjektem 14 ("revizor") Druhého subjektu 2 ("cestující") naváže Čtvrtý subjekt 14 ("revizor") běžným způsobem chráněnou elektronickou komunikaci s Třetím subjektem 3 ("dopravce") využitím Autentizačního systému 8 použitého mezi Čtvrtým subjektem 14 a Třetím subjektem 3 a vytvoří Třetí bezpečný autentizovaný kanál 15. Pomocí Třetího bezpečného autentizovaného kanálu 15 je aktivována Metoda 6 ("biometrická kontrola") Autentizačního objektu 5 ("kontrola") Čtvrtého subjektu 14 zřízeného předtím Třetím subjektem 3 ("dopravce") (který byl zřízen obdobně jako v příkladu 2), pokud je nastaveno právo ji použít.

Metoda 6 ("biometrická kontrola") Autentizačního objektu 5 ("kontrola") Čtvrtého subjektu 14 mimo jiné také připraví ve spolupráci s Rozhraním 10 Autentizačních objektů 5 Třetího subjektu 3 Identifikační informace X1 a Bezpečnostní informace X2 určené k propojení se zařízením kontrolovaného Druhého subjektu 2 ("cestující").

Zařízení Čtvrtého subjektu 14 ("revizor") v součinnosti se zařízením Druhého subjektu 2 ("cestující") a Lokální komunikace 16 mezi zařízením Druhého subjektu 2 ("cestující") a zařízením Čtvrtého subjektu 14 ("revizor") předá Identifikační informace X1 a Bezpečnostní informace X2 např. tím, že zařízení Čtvrtého subjektu 14 ("revizor") zobrazí QR kód pomocí Autentizačního objektu 5 ("kontrola") a Druhý subjekt 2 ("cestující") přečte informaci obsahující Identifikační informace X1 a Bezpečnostní informace X2 pomocí zařízení Druhého subjektu 2 ("cestující") ze zařízení Čtvrtého subjektu 14 ("revizor").

Zařízení Druhého subjektu 2 ("cestující") použije Identifikační informace X1 k navázání chráněné elektronické komunikace se Třetím subjektem 3 ("dopravce") využitím Autentizačního systému 8 použitého mezi zařízením Druhého subjektu 2 a zařízením Třetího subjektu 3 a vytvoří Druhý bezpečný autentizovaný kanál 7. Pomocí Druhého bezpečného autentizovaného kanálu 7 je aktivována Metoda 6 ("biometrická kontrola revizorem") Autentizačního objektu 5 ("jízdenka") Druhého subjektu 2 ("cestující").

Pomocí Identifikačních informací X1 je propojen Druhý bezpečný autentizovaný kanál 7 a Třetí bezpečný autentizovaný kanál 15 v zařízení Třetího subjektu 3 ("dopravce"). Vytvořené Bezpečnostní informace X2, které nebyly přeneseny ze zařízení Druhého subjektu 2 ("cestující") ani ze zařízení Čtvrtého subjektu 14 ("revizor"), mohou být použity k zajištění bezpečnosti, zejména důvěrnosti přenosu dat mezi zařízením Druhého subjektu 2 ("cestující") a zařízením Čtvrtého subjektu 14 ("revizor").

Čtvrtý subjekt 14 ("revizor") pomocí Metody 6 ("biometrická kontrola") Autentizačního objektu 5 ověří interní data X5 pro budoucí použití získané součinností s Metodou 6 ("biometrická kontrola revizorem") Autentizačního objektu 5 ("jízdenka") Druhého subjektu 2 ("cestující") a s Informačním systémem 12 Třetího subjektu 3 ("dopravce") včetně využití zabezpečeného přenosu biometrických dat potřebných ke kontrole ze zařízení Druhého subjektu 2 ("cestující") např. fotografie předtím při nákupu jízdenky podepsané dopravcem.

Potom revizor může provést příslušné kontroly porovnáním biometrických dat s realitou např. pomocí porovnání tváře kontrolovaného cestujícího a fotografií.

Dle Obr. 7.

V případě vstupní kontroly např. u vstupní brány dopravního prostředku vybavené prostředky pro verifikaci biometrických údajů je Lokální komunikací 16 předána Identifikační informace X1 a Bezpečnostní informace X2 mezi Dalším subjektem 20 ("zařízení dopravce") a zařízením Druhého subjektu 2 např. zobrazením QR kódu vstupní branou a sejmutím QR kódu pomocí zařízení Druhého subjektu 2. Další subjekt 20 ("zařízení dopravce") je vůči zařízení Druhého subjektu 2 ("cestující") použit způsobem jako by šlo o zařízení Čtvrtého subjektu 14, tedy způsobem analogickým jako v předchozím textu.

Interní data X5 pro budoucí použití, např. biometrické údaje, předané ze zařízení Druhého subjektu 2 ("cestující") do Dalšího subjektu 20 např. do vstupní brány dopravního prostředku vybavené prostředky pro verifikaci biometrických údajů jsou po ověření pravosti použity k verifikaci reálně sejmutých biometrických údajů např. sejmutého obrazu obličeje.

Při tom může Další subjekt 20 ("zařízení dopravce") spolupracovat také s Informačním systémem 12 Třetího subjektu 3 ("dopravce") a využít výsledků autentizace zařízení Druhého subjektu 2 ("cestující") provedené při vzniku Druhého bezpečného autentizovaného kanálu 7 a interní data X5 pro budoucí použití uložených v Autentizačním objektu 5 ("jízdenka").

Příklad 4 - Vydávání a kontrola osobního elektronického průkazu či osvědčení

Využívá způsob "Založení a konfigurace autentizačního objektu", způsob "Chráněná současná komunikace mezi třemi nebo více subjekty" a způsob "Chráněná komunikace mezi dvěma subjekty přes třetí subjekt navázaná při využití lokální komunikace".

Dle Obr. 8.

Druhý subjekt 2 ("občan") získá od Prvního subjektu 1 ("vydávající instituce") identifikační doklad či jiný průkaz (kvalifikační, členský atd.) na základě příslušného verifikačního procesu, např. ověření občanství, ověření příslušné kvalifikace (např. řidičský průkaz) či naplnění jiných podmínek (např. průkaz zdravotního či sociálního pojištění, členský průkaz).

Elektronická forma průkazu je realizována jako Autentizační objekt 5 ("průkaz") Druhého subjektu 2 ("občan") tak, že zařízení Druhého subjektu 2 ("občan") spolu se zařízením Prvního subjektu 1 ("vydávající organizace") vytvoří pomocí Autentizačního systému 8 První bezpečný autentizovaný kanál 4 mezi Prvním subjektem 1 a Druhým subjektem 2. První subjekt 1 ("vydávající organizace") vytvoří pomocí Prvního bezpečného autentizovaného kanálu 4 nový Autentizační objekt 5 ("průkaz") Druhého subjektu 2 ("občan") včetně stanovení přístupových práv k Metodám 6 Autentizačního objektu 5.

Potřebné osobní údaje a biometrická data potřebná k následné kontrole jako součást interních dat X5 pro budoucí použití jsou uložena v Autentizačním objektu 5 ("průkaz") na zařízení Druhého subjektu 2 ("občan") a mohou být kryptograficky zajištěna proti neoprávněnému použití např. proti modifikaci pomocí elektronického podpisu Prvního subjektu 1 ("vydávající instituce").

V případě ověření správnosti a příslušnosti údajů při vydávání pracovníkem Prvního subjektu 1 ("vydávající instituce") tj. Čtvrtým subjektem 14 ("úředník") naváže Čtvrtý subjekt 14 ("úředník") běžným způsobem chráněnou elektronickou komunikaci se zařízením Prvního subjektu 1 ("vydávající instituce") využitím Autentizačního systému 8 použitého mezi Čtvrtým subjektem 14 ("úředník") a Prvním subjektem 1 ("vydávající instituce") a vytvoří

Čtvrtý bezpečný autentizovaný kanál 17. Pomocí Čtvrtého bezpečného autentizovaného kanálu 17 je aktivována Metoda 6 ("ověřené vydání průkazu") Autentizačního objektu 5 ("vydávání průkazů") Čtvrtého subjektu 14 ("úředník") zřízeného předtím Prvního subjektem 1 ("vydávající instituce") (který byl zřízen např. při pověření úředníka výkonem funkce), pokud je nastaveno právo Metodu 6 ("ověřené vydání průkazu") Autentizačního objektu 5 použít.

Dále pak zařízení Druhého subjektu 2 ("občan") spolu se zařízením Prvního subjektu 1 ("vydávající instituce") vytvoří pomocí Autentizačního systému 8 První bezpečný autentizovaný kanál 4 mezi První subjektem 1 a Druhým subjektem 2. První subjekt 1 ("vydávající instituce") vytvoří pomocí Prvního bezpečného autentizovaného kanálu 4 nový Autentizační objekt 5 ("průkaz") na zařízení Druhého subjektu 2 ("občan"). U tohoto Autentizačního objektu 5 nastaví pravidla řízení přístupu k Metodám objektu 6 tak, že umožní použití Metody 6 ("zkontroluj identitu") Autentizačního objektu 5 pro další subjekty ("kontrolní instituce").

Dále První subjekt 1 ("vydávající instituce") pomocí Metody 6 ("vytvoř Identifikační informace X1 pro vydání") Autentizačního objektu 5 vyžádá vytvoření unikátních Identifikačních informací X1 a Bezpečnostních informací X2 Autentizačním objektem 5 ("průkaz") na zařízení Druhého subjektu 2 ("občan") pro účely propojení se zařízením Čtvrtým subjektem 14 ("úředník") při vydání průkazu s ověřením.

Zařízení Čtvrtého subjektu 14 v součinnosti se zařízením Druhého subjektu 2 a Lokální komunikace 16 mezi zařízením Druhého subjektu 2 ("občan") a zařízením Čtvrtého subjektu 14 ("úředník") předá Identifikační informace X1 a Bezpečnostní informace X2 např. tím, že zařízení Druhého subjektu 2 ("občan") zobrazí QR kód pomocí Autentizačního objektu 5 ("vytvoř Identifikační informace X1 pro vydání") a zařízení Čtvrtého subjektu 14 ("úředník") přečte Identifikační informace X1 a Bezpečnostní informace X2.

Zařízení Čtvrtého subjektu 14 ("úředník") použije tyto Identifikační informace X1 a Bezpečnostní informace X2 jako vstup pro Metodu 6 ("ověřené vydání průkazu") Autentizačního objektu 5 ("vydávání průkazů") Čtvrtého subjektu 14 ("úředník").

Pomocí Identifikačních informací X1 je propojen První bezpečný autentizovaný kanál 4 a Čtvrtý bezpečný autentizovaný kanál 17 v zařízení Prvního subjektu 1 ("vydávající instituce"). Vytvořené Bezpečnostní informace X2, které nebyly přeneseny ze zařízení Druhého subjektu 2 ("občan") ani ze zařízení Čtvrtého subjektu 14 ("úředník"), mohou být použity k zajištění bezpečnosti, zejména důvěrnosti přenosu dat mezi oběma zařízeními.

Čtvrtý subjekt 14 ("úředník") pomocí Metody 6 ("ověřené vydání průkazu") Autentizačního objektu 5 v součinnosti s Metodou 6 ("záznam průkazu") Autentizačního objektu 5 ("průkaz") Druhého subjektu 2 ("občan") a s Informačním systémem 11 Prvního subjektu 1 ("vydávající instituce") zapíše ověřené informace včetně zabezpečeného přenosu biometrických dat na zařízení Druhého subjektu 2 ("občan") např. digitální fotografie, datová podoba otisků prstů, identifikační údaje průkazu, bezpečnostní prvky, informace o platnosti.

Dle Obr. 3.

V případě kontroly fyzickou osobou např. kontroly identity Čtvrtým subjektem 14 ("policista") Druhého subjektu 2 ("občan") naváže Čtvrtý subjekt 14 ("policista") běžným způsobem chráněnou elektronickou komunikaci s Třetím subjektem 3 ("policie") využitím Autentizačního systému 8 použitého mezi Třetím subjektem 3 a Čtvrtým subjektem 14 a vytvoří Třetí bezpečný autentizovaný kanál 15. Pomocí Třetího bezpečného autentizovaného kanálu 15 je aktivována Metoda 6 ("biometrická kontrola") Autentizačního objektu 5 ("kontrola") Čtvrtého subjektu 14 ("policista") zřízeného předtím Třetím subjektem 3 ("policie"), pokud je nastaveno právo Metodu 6 ("biometrická kontrola") Autentizačního objektu 5 použít.

Metoda 6 ("biometrická kontrola") Autentizačního objektu 5 mimo jiné také připraví Identifikační informace X1 a Bezpečnostní informace X2 určené k propojení se zařízením kontrolovaného Druhého subjektu 2 ("občan").

Zařízení Čtvrtého subjektu 14 v součinnosti se zařízením Druhého subjektu 2 a Lokální komunikace 16 mezi zařízením Druhého subjektu 2 ("občan") a zařízením Čtvrtého subjektu 14 ("policista") předá Identifikační informace X1 a Bezpečnostní informace X2 např. tím, že zařízení Čtvrtého subjektu 14 ("policista") zobrazí QR kód pomocí Autentizačního objektu 5 ("kontrola") a Druhý subjekt 2 ("občan") přečte informaci pomocí zařízení Druhého subjektu 2 ("občan") ze zařízení Čtvrtého subjektu 14 ("policista").

Zařízení Druhého subjektu 2 ("občan") použije tyto Identifikační informace X1 k navázání chráněné elektronické komunikace s Třetím subjektem 3 ("policie") využitím Autentizačního systému 8 použitého mezi Druhým subjektem 2 a Třetím subjektem 3 a vytvoří Druhý bezpečný autentizovaný kanál 7. Pomocí Druhého bezpečného autentizovaného kanálu 7 je po ověření přístupových práv Třetího subjektu 3 ("policie") a Čtvrtého subjektu 14 ("policista") aktivována Metoda 6 ("biometrická kontrola policistou") Autentizačního objektu 5 ("průkaz") Druhého subjektu 2 ("občan").

Pomocí Identifikačních informací X1 je propojen Druhý bezpečný autentizovaný kanál 7 a Třetí bezpečný autentizovaný kanál 15. Vytvořené Bezpečnostní informace X2, které nebyly přeneseny ze zařízení Druhého subjektu 2 ("občan") ani ze zařízení Čtvrtého subjektu 14 ("policista"), mohou být použity k zajištění bezpečnosti, zejména důvěrnosti přenosu dat mezi zařízením Druhého subjektu 2 ("občan") a zařízením Čtvrtého subjektu 14 ("policista").

Čtvrtý subjekt 14 ("policista") pomocí Metody 6 ("biometrická kontrola") Autentizačního objektu 5 ("kontrola") ověří informace získané součinností s Metodou 6 ("biometrická kontrola policistou") Autentizačního objektu 5 ("průkaz") Druhého subjektu 2 ("občan") a ve spolupráci s Informačním systémem 12 Třetího subjektu 3 ("policie") včetně zabezpečeného přenosu biometrických data potřebných ke kontrole ze zařízení Druhého subjektu 2 ("občan") např. fotografie předtím při vydání průkazu podepsanou Prvním subjektem 1 ("vydávající instituce") (dle obr. 8) provede kontrolu např. pomocí porovnání tváře kontrolovaného občana a fotografií získanou z elektronického průkazu, ověřením nenarušení údajů a platnosti průkazu.

Dle Obr. 5.

Při kontrole může být také využita komunikace mezi Informačním systémem 11 Prvního subjektu 1 ("vydávající instituce") a Informačním systémem 12 třetího subjektu 3 ("policie") zajištěná běžnými prostředky komunikace mezi informačními systémy.

Dle Obr. 7.

V případě automatizované kontroly fyzické identity občana (např. vstupní brány budov, automatizovaná hraniční kontrola) Třetím subjektem 3 ("kontrolní instituce") vybaveným Dalším subjektem 20 ("kontrolní zařízení") obsahujícím prostředky pro verifikaci biometrických údajů je Lokální komunikací 16 předána Identifikační informace X1 a Bezpečnostní informace X2 mezi Dalším subjektem 20 a zařízením Druhého subjektu 2 ("občan") např. zobrazením QR kódu vstupní branou a sejmutím QR kódu pomocí zařízení Druhého subjektu 2 nebo pomocí bezdrátového senzoru. Další subjekt 20 ("kontrolní zařízení") je vůči zařízení Druhého subjektu 2 ("občan") použito způsobem jako by šlo o zařízení Čtvrtého subjektu 14, tedy způsobem analogickým jako v příkladu 3.

Na základě Identifikační informace X1 a Bezpečnostní informace X2 předaných z Dalšího subjektu 20 ("kontrolní zařízení") na zařízení Druhého subjektu 2 ("občan") je vytvořen Druhý bezpečný autentizovaný kanál 7 pomocí Autentizačního systému 8 použitého mezi

Druhým subjektem 2 ("občan") a Třetím subjektem 3 ("kontrolní instituce") a pomocí tohoto Druhého bezpečného autentizovaného kanálu 7 vyžádá Třetí subjekt 3 ("kontrolní instituce") provedení Metody 6 ("biometrické ověření identity") Autentizačního objektu 5 ("průkaz") včetně předání případných příslušných parametrů např. požadovaný biometrický prvek (fotografie, otisk prstu,...).

Pokud jsou nastavena příslušná práva provedení Metody 6 ("biometrické ověření identity") Autentizačního objektu 5 ("průkaz") pro Třetí subjekt 3 ("kontrolní instituce") komunikuje Metoda 6 ("biometrické ověření identity") Autentizačního objektu 5 ("průkaz") pomocí Druhého bezpečného autentizovaného kanálu 7 s Informačním systémem 12 Třetího subjektu 3.

Dle Obr. 5.

Informační systém 12 Třetího subjektu 3 za případné spolupráce s Informačním systémem 11 Prvního subjektu 1 ("vydávající instituce") zajištěnými běžnými prostředky komunikace mezi informačními systémy provede verifikaci příslušných údajů (např. ověření nenarušení a platnosti údajů) včetně ověření shody biometrických dat.

Biometrické údaje předané ze zařízení Druhého subjektu 2 ("občan") do Dalšího subjektu 20 ("kontrolní zařízení") např. do systému automatizované hraniční kontroly vybavené prostředky pro verifikaci biometrických údajů jsou po ověření pravosti použity k verifikaci reálně sejmutých biometrických údajů např. sejmutého obrazu obličeje či sejmutých otisků prstů.

Při tom může Další subjekt 20 ("kontrolní zařízení") spolupracovat také s Informačním systémem 12 Třetího subjektu 3 ("kontrolní instituce") a také s Informačním systémem 11 Prvního subjektu 1 ("vydávající instituce") a využít výsledků autentizace zařízení Druhého subjektu 2 ("občan") a informací uložených v Autentizačním objektu 5 ("průkaz").

Dle Obr. 5.

Je také možné, aby na základě Identifikační informace X1 a Bezpečnostní informace X2 předaných z Dalšího subjektu 20 ("kontrolní zařízení") na zařízení Druhého subjektu 2 ("občan") byl vytvořen současně také První bezpečný autentizovaný kanál 4 pomocí Autentizačního systému 8 použitého mezi Druhým subjektem 2 ("občan") a Prvním subjektem 1 ("vydávající organizace") a pomocí tohoto Prvního bezpečného autentizovaného kanálu 4 probíhala komunikace Dalšího subjektu 20 nebo Informačního systému 12 Třetího

subjektu 3 ("kontrolní instituce") s Informačním systémem 11 Prvního subjektu 1 ("vydávající instituce").

Příklad 5 Pasivní označovač - vstupní brány, prokázání přítomnosti, označení jízdenky

Využívá způsob "Založení a konfigurace autentizačního objektu" a způsob "Spuštění metody autentizačního objektu konstantní lokální komunikací".

Dle Obr. 1.

Druhý subjekt 2 ("uživatel") spolu s Prvním subjektem 1 ("provozovatel") vytvoří pomocí Autentizačního systému 8, který má Serverovou část 8a Autentizačního systému 8 a Klientskou část 8b Autentizačního systému 8, První bezpečný autentizovaný kanál 4 mezi První subjektem 1 a Druhým subjektem 2. První subjekt 1 ("provozovatel") vytvoří pomocí Prvního bezpečného autentizovaného kanálu 4 nový Autentizační objekt 5 ("pasivní označovač") na zařízení Druhého subjektu 2 ("uživatel"). U tohoto Autentizačního objektu 5 nastaví pravidla řízení přístupu k Metodám 6 Autentizačního objektu 5 tak, že umožňují použití Metody 6 Autentizačního objektu 5 pro další subjekty. Dále První subjekt 1 ("provozovatel") také nastaví Spouštěcí informace X3 pro lokální spuštění příslušné Metody 6 Autentizačního objektu 5. První bezpečný autentizovaný kanál 4 se uzavře.

Dle Obr. 4.

Druhý subjekt 2 ("uživatel") sejme užitím Lokální komunikace 16 z pasivního prvku pevnou Sejmutou informaci X4 obsahující parametr a hodnotu charakterizující potřebnou akci a její parametry jako je označení brány např. pro zjištění průchodu místem, otevření brány, označení jízdenky, apod. Může použít různé formy Lokální komunikace 16 např. např. vyfotografování vytištěného QR kódu, bezdrátovou komunikaci, zvukovou komunikaci či jinou formu optické komunikace.

Zařízení Druhého subjektu 2 ("uživatel") podle Sejmuté informace X4 aktivuje příslušnou Metodu 6 Autentizačního objektu 5 ("pasivní označovač").

Metoda 6 Autentizačního objektu 5 pomocí Autentizačního systému 8 vytvoří První bezpečný autentizovaný kanál 4 mezi zařízením Prvního subjektu 1 a zařízením Druhého subjektu 2, případně jiný bezpečný kanál mezi zařízením Druhého subjektu 2 a jiným Dalším subjektem

20 podle dříve nastavené konfigurace Autentizačního objektu 5 ("pasivní označovač") a podle obsahu sejmuté informace.

Metoda 6 Autentizačního objektu 5 provede případně spolu s Informačním systémem 11 Prvního subjektu 1 nebo/a spolu s dalšími zařízeními či systémy příslušnou akci, např. zaznamená čas a informace o místě označení do elektronické jízdenky, otevře či neotevře příslušnou bránu, označí průchod místem atd.

Příklad 6 – přenos osobních informací mezi subjekty

Využívá způsob „Založení a konfigurace autentizačního objektu“ a způsob „Chráněná současná komunikace mezi třemi nebo více subjekty“.

Dle Obr. 2.

Druhý subjekt 2 ("uživatel") spolu s Prvním subjektem 1 ("poskytovatel identity") vytvoří pomocí Autentizačního systému 8 První bezpečný autentizovaný kanál 4 mezi První subjektem 1 a Druhým subjektem 2. První subjekt 1 ("poskytovatel identity") vytvoří pomocí Prvního bezpečného autentizovaného kanálu 4 nový Autentizační objekt 5 ("zaručená identita") na zařízení Druhého subjektu 2 ("uživatel"). U tohoto Autentizačního objektu 5 nastaví pravidla řízení přístupu k Metodám 6 ("zaručená identita") Autentizačního objektu 5 tak, že umožní použití Metody 6 ("předej osobní údaje") Autentizačního objektu 5 pro další subjekty ("příjemce identity").

V době kdy Druhý subjekt 2 ("uživatel") komunikuje vzdáleně se Třetím subjektem 3 ("příjemce identity") a chce umožnit předání osobních údajů ověřených dříve Prvním subjektem 1 ("poskytovatel identity") je už vytvořen nebo se vytvoří Druhý bezpečný autentizovaný kanál 7 pomocí Autentizačního systému 8, který má Serverovou část 8a Autentizačního systému 8 a Klientskou část 8b Autentizačního systému 8, použitého mezi zařízením Druhého subjektu 2 ("uživatel") a zařízením Třetího subjektu 3 ("příjemce identity") a pomocí tohoto Druhého bezpečného autentizovaného kanálu 7 vyžádá Třetí subjekt 3 ("příjemce identity") provedení Metody 6 ("předej osobní údaje") Autentizačního objektu 5 ("zaručená identita") včetně předání příslušných parametrů jako je např. seznam požadovaných osobních údajů.

Požadavek předání osobních údajů ve formě požadavku na provedení ("předej osobní údaje") Autentizačního objektu 5 ("zaručená identita") jsou přeneseny například z Informačního

systému 12 Třetího subjektu 3 do Rozhraní 10 Autentizačních objektů 5 Třetího subjektu 3 a dále vytvořeným Druhým bezpečným autentizovaným kanálem 7 mezi Třetím subjektem 3 ("příjemce identity") a Druhým subjektem 2 ("uživatel") do zařízení Druhého subjektu 2 ("uživatel").

Druhý subjekt 2 ("uživatel") vyhodnotí nastavená přístupová pravidla Metody 6 ("předej osobní údaje") Autentizačního objektu 5 pro konkrétní Třetí subjekt 3 ("příjemce identity") a v případě shody pokračuje ve zpracování. V případě neshody zpracování požadavku zpracování odmítne.

Pokud zpracování pokračuje, vytvoří Metoda 6 ("předej osobní údaje") Autentizačního objektu 5 ("zaručená identita") s pomocí Autentizačního systému 8 První bezpečný autentizovaný kanál 4 mezi Druhým subjektem 2 ("uživatel") a Prvním subjektem 1 ("poskytovatel identity"), který existuje současně s Druhým bezpečným autentizovaným kanálem 7 mezi Druhým subjektem 2 ("uživatel") a Třetím subjektem 3 ("příjemce identity"). Pomocí Prvního bezpečného autentizovaného kanálu 4 a Rozhraní 9 Autentizačních objektů 5 Prvního subjektu 1 jsou přenášeny zprávy mezi Autentizačním objektem 5 ("zaručená identita") a Informačním systémem 11 Prvního subjektu 1 potřebné k předání vyžádaných osobních údajů včetně potřebného potvrzování uživatelem. Po úspěšném provedení či po odmítnutí Prvním subjektem 1 ("poskytovatel identity") či Druhým subjektem 2 ("uživatel") je výsledek a případně další informace přenesen pomocí Druhého bezpečného autentizovaného kanálu 7 mezi Druhým subjektem 2 ("uživatel") a Třetím subjektem 3 ("příjemce identity") například do Informačního systému 12 Třetího subjektu 3.

Příklad 7 – potvrzování plateb a jiných transakcí

Využívá způsob "Založení a konfigurace autentizačního objektu" a způsob "Spuštění metody Autentizačního objektu konstantní lokální komunikací".

Dle Obr. 1.

Druhý subjekt 2 ("uživatel") spolu s Prvním subjektem 1 např. ("banka") vytvoří pomocí Autentizačního systému 8 První bezpečný autentizovaný kanál 4 mezi První subjektem 1 a Druhým subjektem 2. První subjekt 1 ("banka") vytvoří pomocí Prvního bezpečného autentizovaného kanálu 4 nový Autentizační objekt 5 např. ("platební modul") na zařízení Druhého subjektu 2 ("uživatel"). U tohoto Autentizačního objektu 5 ("platební modul")

nastaví pravidla řízení přístupu k Metodám 6 Autentizačního objektu 5 tak, že umožní použití Metody 6 ("zaplať") Autentizačního objektu 5 pro další subjekty.

Dle Obr. 1 + Obr. 4.

Dále První subjekt 1 ("banka") nastaví také Spouštěcí informace X3 pro lokální spuštění příslušné metody nebo metod např. nastaví Spouštěcí informace X3 pro Metodu 6 ("zaplať") Autentizačního objektu 5 tak aby metoda byla aktivována pomocí Lokální komunikace 16, např. vyfotografováním QR kódu obsahujícího informace o platbě nebo složenky či šeku nebo stlačením příslušného tlačítka na zařízení Druhého subjektu 2 ("uživatel").

Jiný subjekt případně První subjekt 1 vytvoří příslušné Sejmuté informace X4 - podklady pro provedení platby či pro potvrzení jiné transakce, např. zobrazí QR kód na webové stránce svého informačního systému, vytiskne a zašle složenku, připraví platební příkaz na základě telefonického hovoru Druhého subjektu 2 ("uživatel") s call centrem.

Dle Obr. 4.

Později, když Druhý subjekt 2 ("uživatel") sejme užitím Lokální komunikace 16 nastavenou Sejmutou informaci X4 např. tím, že vyfotografuje na obrazovce zobrazený QR kód nebo vyfotografuje vytištěný QR kód, vyfotografuje složenku či stiskne příslušné tlačítko, zařízení Druhého subjektu 2 ("uživatel") podle Sejmuté informace X4 aktivuje příslušnou Metodu 6 ("zaplať") Autentizačního objektu 5 ("platební modul").

Autentizační objekt 5 vyhodnotí nastavená přístupová pravidla Metody 6 ("zaplať") Autentizačního objektu 5 pro konkrétní Sejmuté informace X4 a v případě shody se Spouštěcí informací X3 a nastavenými přístupovými právy se pokračuje ve zpracování.

Pokud zpracování pokračuje, vytvoří Metoda 6 ("zaplať") Autentizačního objektu 5 pomocí Autentizačního systému 8 První bezpečný autentizovaný kanál 4 mezi Prvním subjektem 1 ("banka") a Druhým subjektem 2 ("uživatel"), případně jiný bezpečný kanál mezi Druhým subjektem 2 ("uživatel") a jiným subjektem podle dříve nastavené konfigurace Autentizačního objektu 5 a Sejmuté informace X4.

Pomocí Prvního bezpečného autentizovaného kanálu 4 a Rozhraní 9 Autentizačních objektů 5 Prvního subjektu 1 jsou přenášeny zprávy mezi Autentizačním objektem 5 ("platební modul") a Informačním systémem 11 Prvního subjektu 1 potřebné k zadání a potvrzení platby včetně potřebného potvrzování uživatelem a kryptografických operací pomocí dříve vytvořeného kryptografického materiálu.

Analogicky je prováděno potvrzování jiných typů transakcí.

Příklad 8 – ověřování lokálního autentizačního faktoru jiným subjektem

Využívá způsob "Založení a konfigurace autentizačního objektu" a způsob "Chráněná současná komunikace mezi třemi nebo více subjekty".

Dle Obr. 1.

Pojem „lokální autentizační faktor“ znamená libovolný způsob potvrzování vlastnictví zařízení Druhého subjektu 2 ("uživatel") všeobecně nazývaného např. jako více faktorová autentizace, prováděná lokálně pomocí zařízení Druhého subjektu 2 ("uživatel") např. sejmutí a ověření biometrických údajů jako je otisk prstu, obraz obličeje, sítnice, sejmutí cévního systému prstu, zadání tajné informace jako je PIN, heslo, aktivační sekvence obrázků.

Druhý subjekt 2 ("uživatel") spolu s Prvním subjektem 1 ("poskytovatel identity") vytvoří pomocí Autentizačního systému 8 První bezpečný autentizovaný kanál 4 mezi zařízením Prvního subjektu 1 ("uživatel") a zařízením Druhého subjektem 2 ("poskytovatel identity"). První subjekt 1 ("poskytovatel identity") vytvoří pomocí Prvního bezpečného autentizovaného kanálu 4 nový Autentizační objekt 5 ("správa druhého faktoru") na zařízení Druhého subjektu 2 ("uživatel"). U tohoto Autentizačního objektu 5 nastaví pravidla řízení přístupu k Metodám 6 Autentizačního objektu 5 tak, že umožní použití Metody 6 ("ověř druhý faktor") Autentizačního objektu 5 pro další subjekty ("příjemce identity").

Druhý subjekt 2 ("uživatel") za podmínek určených Prvním subjektem 1 ("poskytovatel identity") použije druhý faktor na zařízení Druhého subjektu 2 ("uživatel") spolu s použitím Metody 6 ("nastav druhý faktor") Autentizačního objektu 5. Metoda 6 ("nastav druhý faktor") Autentizačního objektu 5 pomocí Prvního bezpečného autentizovaného kanálu 4 s užitím známých kryptografických metod (např. asymetrická kryptografie, hash funkce, "zero knowledge proof") zařízením Druhého subjektu 2 ("uživatel") a zařízením Prvního subjektu 1 ("poskytovatel identity") přenese potřebné informace a zaznamená kryptografický důkaz užitého druhého faktoru na zařízení Prvního subjektu 1 ("poskytovatel identity"). Použité kryptografické metody mohou zaručit, že důkaz druhého faktoru lze použít k ověření správnosti druhého faktoru, ale nelze z něj druhý faktor zrekonstruovat.

Dle Obr. 2.

V době kdy Druhý subjekt 2 ("uživatel") komunikuje vzdáleně se Třetím subjektem 3 ("příjemce identity") a chce umožnit ověření správnosti druhého faktoru dříve ověřeného Prvním subjektem 1 ("poskytovatel identity") je už vytvořen nebo se vytvoří Druhý bezpečný autentizovaný kanál 7 pomocí Autentizačního systému 8 použitého mezi zařízením Druhého subjektu 2 ("uživatel") a zařízením Třetího subjektu 3 ("příjemce identity") a pomocí tohoto Druhého bezpečného autentizovaného kanálu 7 vyžádá Třetí subjekt 3 ("příjemce identity") provedení Metody 6 ("ověř druhý faktor") Autentizačního objektu 5 ("správa druhého faktoru").

Zařízením Druhého subjektu 2 ("uživatel") vyhodnotí nastavená přístupová pravidla Metody 6 ("ověř druhý faktor") Autentizačního objektu 5 ("správa druhého faktoru") pro konkrétní Třetí subjekt 3 ("příjemce identity") a v případě shody pokračuje ve zpracování. V případě neshody zpracování požadavku na požadavek odmítne.

Pokud zpracování pokračuje, vytvoří Metoda 6 ("ověř druhý faktor") Autentizačního objektu 5 ("správa druhého faktoru") s pomocí Autentizačního systému 8 První bezpečný autentizovaný kanál 4 mezi Druhým subjektem 2 ("uživatel") a Prvním subjektem 1 ("poskytovatel identity"), který existuje současně s Druhým bezpečným autentizovaným kanálem 7 mezi Druhým subjektem 2 ("uživatel") a Třetím subjektem 3 ("příjemce identity"). Při tom Metoda 6 ("ověř druhý faktor") Autentizačního objektu 5 vyžádá použití lokálního autentizačního faktoru zařízením Druhého subjektu 2 ("uživatel") např. sejmutí otisku prstu nebo zadání tajné informace. Užitím známých kryptografických metod (např. asymetrická kryptografie, hash funkce, „zero knowledge proof“) zařízením Druhého subjektu 2 ("uživatel") a zařízením Prvního subjektu 1 ("poskytovatel identity") jsou předány informace k ověření kryptografického důkazu správnosti druhého faktoru prostřednictvím Prvního bezpečného autentizovaného kanálu 4 zařízení Prvního subjektu 1 ("poskytovatel identity"), které s užitím dříve uloženého kryptografického důkazu užitého druhého faktoru zařízení Prvního subjektu 1 ("poskytovatel identity") vyhodnotí.

Výsledek ověření lokálního autentizačního faktoru Prvním subjektem 1 ("poskytovatel identity") je přenesen pomocí Prvního bezpečného autentizovaného kanálu 4 a Druhého bezpečného autentizovaného kanálu 7 mezi Prvním subjektem 1 ("poskytovatel identity") a Třetím subjektem 3 ("příjemce identity").

Příklad 9 – vytvoření repliky

Využívá způsob "Založení a konfigurace autentizačního objektu" a způsob "Chráněná komunikace mezi dvěma subjekty přes třetí subjekt navázaná při využití lokální komunikace".

Dle Obr. 6.

Uživatel je vybaven dvěma zařízeními a to Prvním zařízením uživatele 21 a Druhým zařízením uživatele 22. Uživatel chce na Druhém zařízení uživatele 22 vytvořit repliku Prvního zařízení uživatele 21 bezpečným způsobem, tedy aby bylo bezpečně ověřeno, že První zařízení uživatele 21 a Druhé zařízení uživatele 22 patří stejnému uživateli. Přitom První zařízení uživatele 21 a Druhé zařízení uživatele 22 budou při elektronické komunikaci bezpečně odlišitelná, tedy nebudou shodná.

Druhý subjekt 2 ("uživatel") s použitím Prvního zařízení uživatele 21 spolu s Prvním subjektem 1 ("poskytovatel elektronické služby") vytvoří pomocí Autentizačního systému 8 První bezpečný autentizovaný kanál 4 mezi Prvním zařízením uživatele 21 a Prvním subjektem 1 ("poskytovatel elektronické služby"). První subjekt 1 ("poskytovatel elektronické služby") vytvoří pomocí Prvního bezpečného autentizovaného kanálu 4 nový Autentizační objekt 5 ("správa repliky") na Prvním zařízení uživatele 21. U tohoto Autentizačního objektu 5 nastaví pravidla řízení přístupu k Metodám 6 Autentizačního objektu 5 tak, že umožní použití Metody 6 ("použij pro repliku") Autentizačního objektu 5 pro První subjekt 1 ("poskytovatel elektronické služby").

V okamžiku kdy Druhý subjekt 2 ("uživatel") chce vytvořit repliku Prvního zařízení uživatele 21 na Druhé zařízení uživatele 22, Druhý subjekt 2 ("uživatel") s použitím Prvního zařízení uživatele 21 spolu s Prvním subjektem 1 ("poskytovatel elektronické služby") vytvoří pomocí Autentizačního systému 8 První bezpečný autentizovaný kanál 4 mezi Prvním zařízením uživatele 21 a Prvním subjektem 1 ("poskytovatel elektronické služby"). První subjekt 1 ("poskytovatel elektronické služby") pomocí Prvního bezpečného autentizovaného kanálu 4, spustí Metodu 6 ("použij pro repliku") Autentizačního objektu 5 ("správa repliky") na Prvním zařízení uživatele 21.

Metoda objektu 6 ("použij pro repliku") pomocí Prvního bezpečného autentizovaného kanálu 4 vytvoří v Rozhraní 10 Autentizačních objektů 5 Replikační ukončení 23.

Metoda 6 ("použij pro repliku") Autentizačního objektu 5 také vytvoří potřebné Identifikační informace X1 a Bezpečnostní informace X2.

Dále Druhý subjekt 2 ("uživatel") s použitím Druhého zařízení uživatele 22 a Lokální komunikace 16 propojí lokálně První zařízení uživatele 21 s Druhým zařízení uživatele 22. Druhé zařízení uživatele 22 přenese připravené Identifikační informace X1 a Bezpečnostní informace X2 z Prvního zařízení uživatele 21 pomocí Lokální komunikace 16.

Druhé zařízení uživatele 22 s využitím Identifikační informace X1 spolu s Prvním subjektem 1 ("poskytovatel elektronické služby") vytvoří pomocí Autentizačního systému 8 Druhý bezpečný autentizovaný kanál 7 mezi Druhým zařízením uživatele 22 a Prvním subjektem 1 ("poskytovatel elektronické služby"). První subjekt 1 ("poskytovatel elektronické služby") pomocí Druhého bezpečného autentizovaného kanálu 7 vytvoří nový Autentizační objekt 5 ("správa repliky") na Druhém zařízení uživatele 22. U tohoto Autentizačního objektu 5 nastaví pravidla řízení přístupu k Metodám 6 Autentizačního objektu 5 tak, že umožní použití Metody 6 ("vytvoř repliku") Autentizačního objektu 5 ("správa repliky") pro První subjekt 1 ("poskytovatel elektronické služby"). Dále spustí Metodu 6 ("vytvoř repliku") Autentizačního objektu 5 ("správa repliky") na Druhém zařízení uživatele 22.

Metoda 6 ("vytvoř repliku") Autentizačního objektu 5 ("správa repliky") zpracuje přenesené Bezpečnostní informace X2 a s využitím přenesené Identifikační informace X1 se s využitím Druhého bezpečného autentizovaného kanálu 7 připojí k Replikačnímu ukončení 23 v Rozhraní 10 Autentizačních objektů 5 Prvního subjektu 1 ("poskytovatel elektronické služby").

Od tohoto okamžiku může První zařízení uživatele 21 komunikovat obousměrně s Druhým zařízením uživatele 22 přes Replikační ukončení 23 v Rozhraní 10 Autentizačních objektů 5 Prvního subjektu 1 ("poskytovatel elektronické služby") při využití Prvního bezpečného autentizovaného kanálu 4 a Druhého bezpečného autentizovaného kanálu 7. Přitom komunikace je chráněna při přenosu přes Obecnou síť 13, která nemusí být zabezpečena, např. pomocí Internetu.

Protože Autentizační objekt 5 ("správa repliky") na Prvním zařízení uživatele 21 a také Autentizační objekt 5 ("správa repliky") na Druhém zařízení uživatele 22 mají k dispozici Bezpečnostní informace X2, přenesené přes Lokální komunikaci 16, může být komunikace Prvního zařízení uživatele 21 s Druhým zařízením uživatele 22 přes Replikační ukončení 23 utajena šifrováním i před Prvním subjektem 1 ("poskytovatel elektronické služby").

Od tohoto okamžiku je také prokázáno, že První zařízení uživatele 21 a také Druhé zařízení uživatele 22 spolu komunikovaly pomocí Lokální komunikace 16 a to lze považovat za

ověření toho, že patří témuž uživateli. To vyznačí První subjekt 1 ("poskytovatel elektronické služby") do svých vnitřních záznamů a tím je replika vytvořena.

PATENTOVÉ NÁROKY

1. Způsob navazování chráněné elektronické komunikace, bezpečného přenášení a zpracování informací mezi třemi a popřípadě více subjekty vyznačující se tím, že se nejprve s pomocí autentizačního systému (8) vytvoří první bezpečný autentizovaný kanál (4) mezi prvním subjektem (1) a druhým subjektem (2), prostřednictvím kterého první subjekt (1) ve spolupráci s druhým subjektem (2) vytvoří autentizační objekt (5) uložený na druhém subjektu (2) a vybavený metodami (6) autentizačního objektu (5), přičemž metody (6) autentizačního objektu (5) nastaví první subjekt (1) tak, že ke každé metodě (6) autentizačního objektu (5) přiřadí informaci o právech alespoň jednoho dalšího subjektu (3, 20), a popřípadě i prvního subjektu (1), používat alespoň jednu metodu (6) autentizačního objektu (5), a první bezpečný autentizovaný kanál (4) se uzavře.

2. Způsob podle nároku 1, vyznačující se tím, že autentizační objekt (5) obsahuje interní data (X5) pro budoucí použití.

3. Způsob podle nároku 1 nebo 2, vyznačující se tím, že následně se s pomocí autentizačního systému (8) vytvoří druhý bezpečný autentizovaný kanál (7) mezi druhým subjektem (2) a třetím subjektem (3), pomocí kterého se aktivuje metoda (6) autentizačního objektu (5), která iniciuje s pomocí autentizačního systému (8) vytvoření prvního bezpečného autentizovaného kanálu (4) mezi druhým subjektem (2) a prvním subjektem (1) nebo jiným subjektem, přičemž první bezpečný autentizovaný kanál (4) existuje současně s druhým bezpečným autentizovaným kanálem (7) a využijí se k následnému zabezpečenému přenášení informací mezi všemi subjekty.

4. Způsob podle nároku 1 nebo 2, vyznačující se tím, že metoda (6) autentizačního objektu (5) vytvoří s pomocí autentizačního systému (8) dva nebo více bezpečných autentizovaných kanálů mezi druhým subjektem (2) a dvěma nebo více dalšími subjekty (1, 3, 20), které existují současně s prvním bezpečným autentizovaným kanálem (4), a všechny takové bezpečné autentizované kanály se společně využijí k následnému zabezpečenému přenášení informací mezi všemi subjekty.

5. Způsob dle nároku 1 nebo 2, vyznačující se tím, že první subjekt (1) vytvoří nezávisle na sobě autentizační objekty (5) vybavené metodami (6) těchto autentizačních objektů (5) druhému subjektu (2) a čtvrtému subjektu (14), přičemž druhý subjekt (2) a první subjekt (1) mezi sebou následně s pomocí autentizačního systému (8) vytvoří první bezpečný autentizovaný kanál (4), pomocí kterého se aktivuje metoda (6) autentizačního objektu (5) druhého subjektu (2), která připraví ve spolupráci s prvním subjektem (1) identifikační informace (X1) určené k propojení druhého subjektu (2) se čtvrtým subjektem (14) a také bezpečnostní informace (X2) určené k následnému zabezpečení komunikace mezi druhým subjektem (2) a čtvrtým subjektem (14), přičemž identifikační informace (X1) a bezpečnostní informace (X2), které jsou známy pouze druhému subjektu (2), se z druhého subjektu (2) přenesou na čtvrtý subjekt (14) a následně se mezi prvním subjektem (1) a čtvrtým subjektem (14) s pomocí autentizačního systému (8) vytvoří čtvrtý bezpečný autentizovaný kanál (17), který se pomocí identifikačních informací (X1) propojí s prvním bezpečným autentizovaným kanálem (4), a bezpečnostní informace (X2) použijí se k následnému zabezpečenému přenášení informací mezi druhým subjektem (2) a čtvrtým subjektem (14) prostřednictvím prvního subjektu (1).

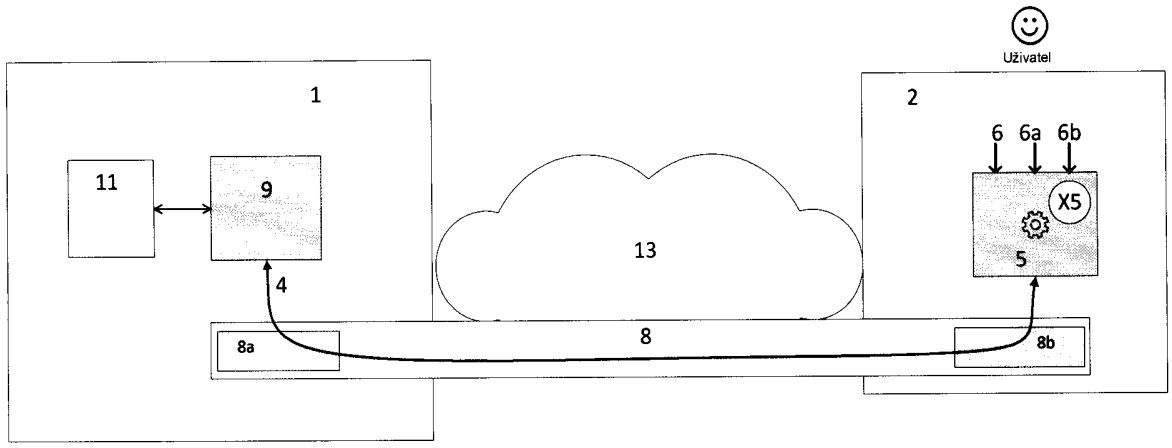
6. Způsob podle nároku 5, vyznačující se tím, že identifikační informace (X1) a bezpečnostní informace (X2) se přenesou z druhého subjektu (2) na čtvrtý subjekt (14) pomocí lokální komunikace (16).

7. Způsob podle nároku 2, vyznačující se tím, že v rámci interních dat (X5) pro budoucí použití autentizačního objektu (5) se na druhém subjektu (2) nastaví spouštěcí informace (X3) pro lokální spuštění metody (6) autentizačního objektu (5), která se následně spustí samotným druhým subjektem (2) nebo pomocí lokální komunikace (16) s jedním nebo více jinými zařízeními obsahujícími sejmutou informaci (X4), která spouštěcí informaci (X3) odpovídá předem zvoleným způsobem, přičemž po svém spuštění metoda (6) autentizačního objektu (5) s využitím interních dat (X5) pro budoucí použití a s pomocí autentizačního systému (8) vytvoří jeden nebo více autentizovaných kanálů (4), které se použijí k následnému zabezpečenému přenášení informací mezi druhým subjektem (2) a jedním nebo více dalších subjektů (20) dle konfigurace autentizačního objektu (5).

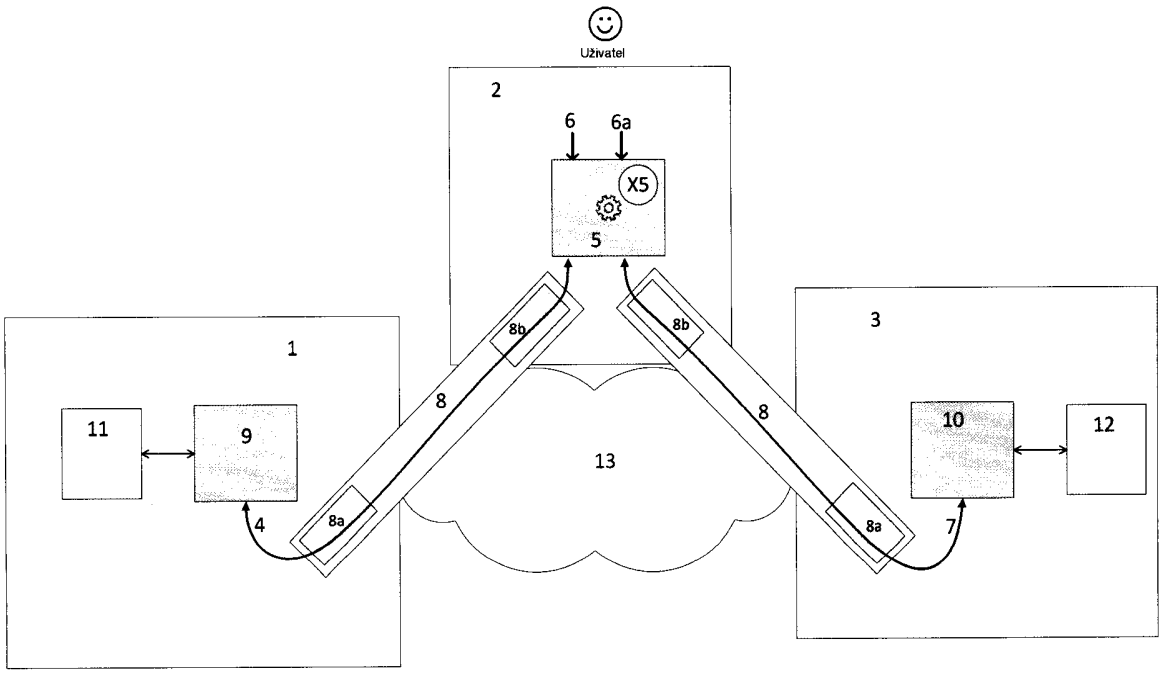
8. Způsob podle nároku 7, vyznačující se tím, že metoda (6) autentizačního objektu (5) využije sejmutou informaci (X4).

PV 2015-472
07.07.15

Obr.1

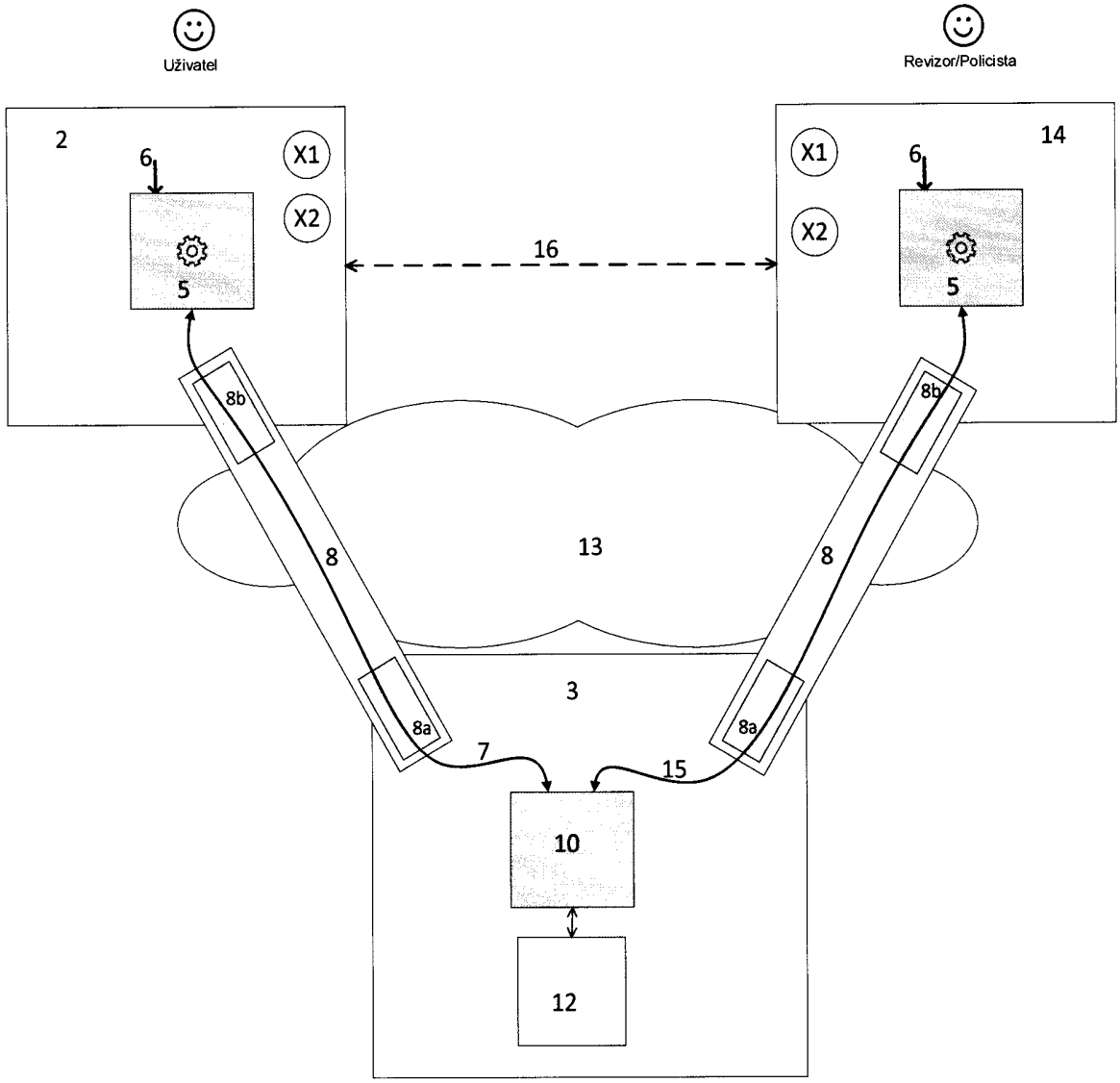


Obr.2



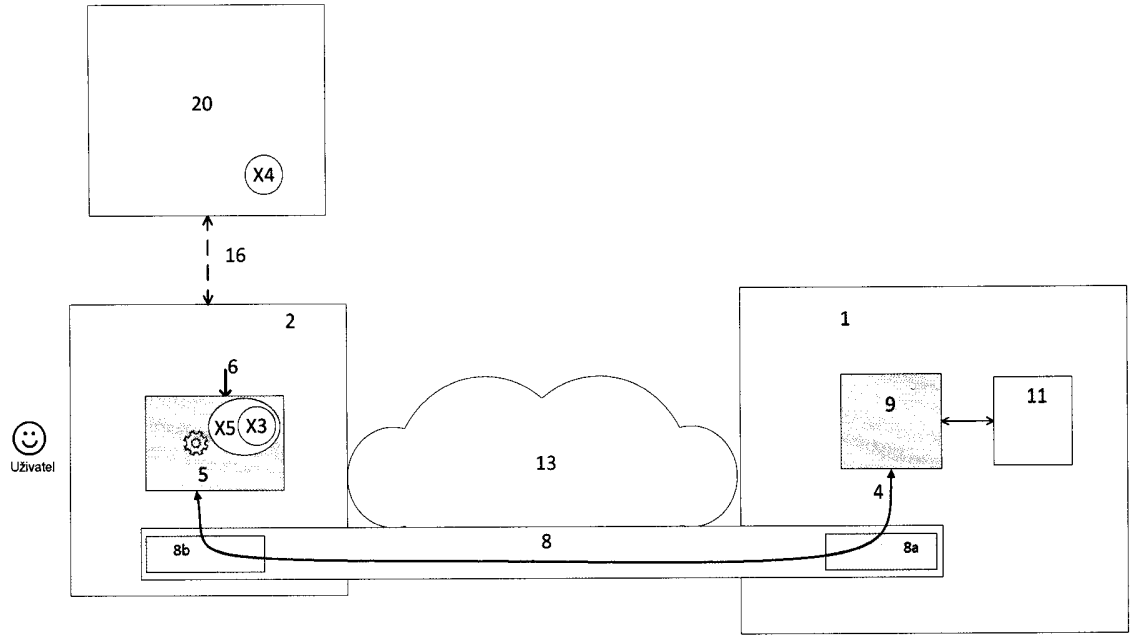
07.07.15

Obr.3

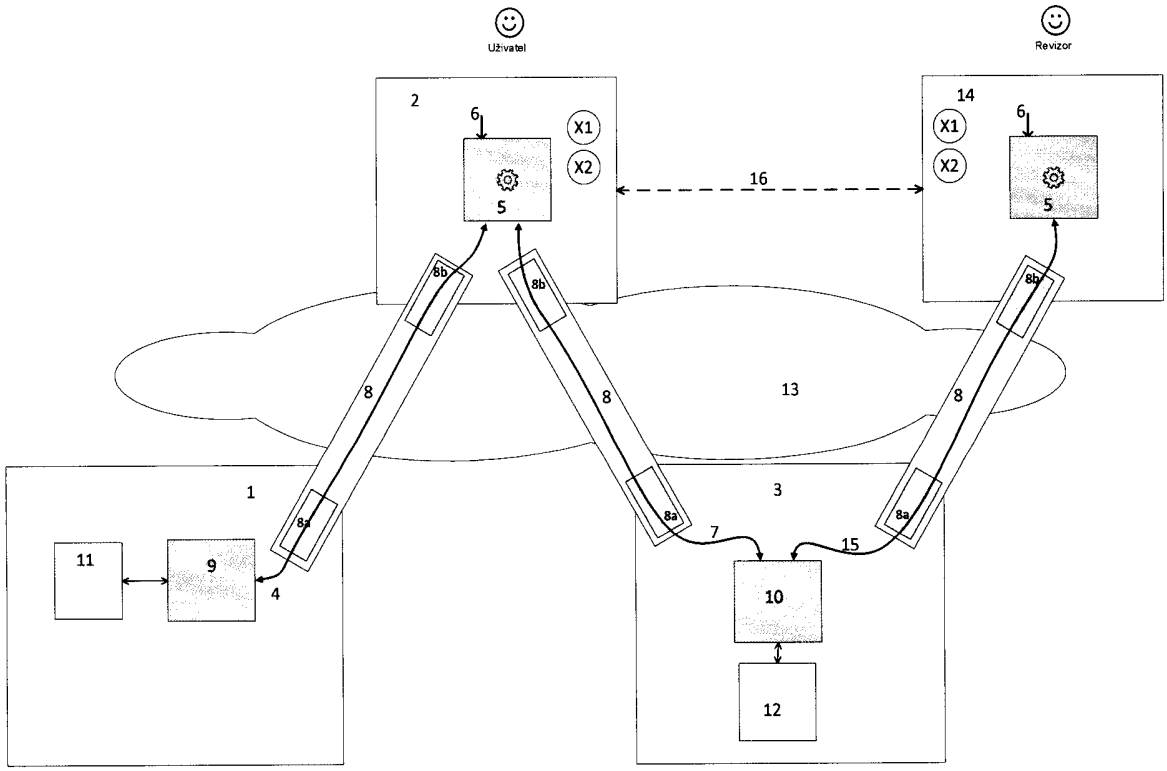

Uživatel
Revizor/Policista
2
6
X1
X2
5
16
14
X1
X2
6
5
8b
8b
8
8
13
3
8a
8a
7
15
10
12

07.07.15

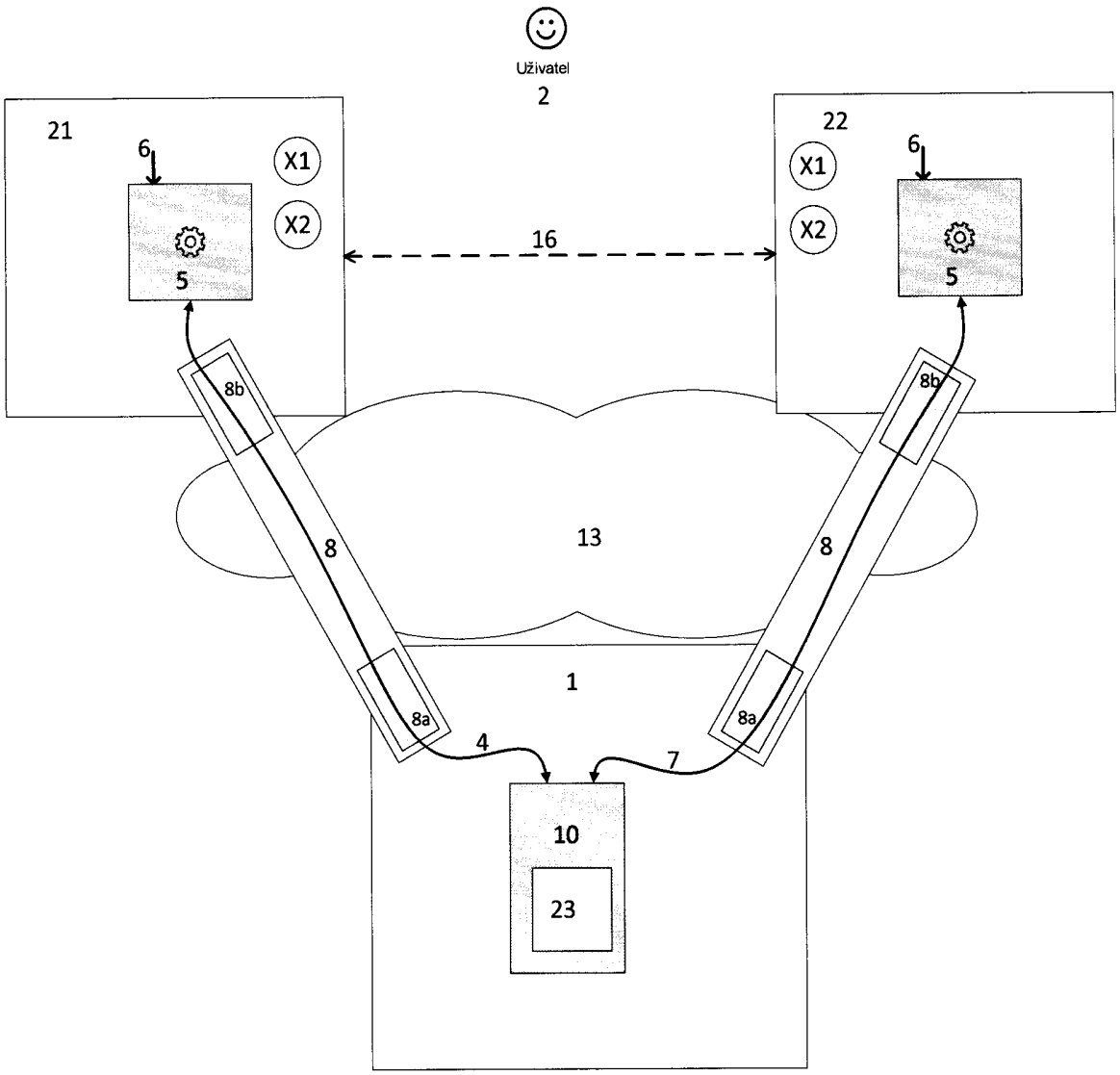
Obr.4



Obr.5

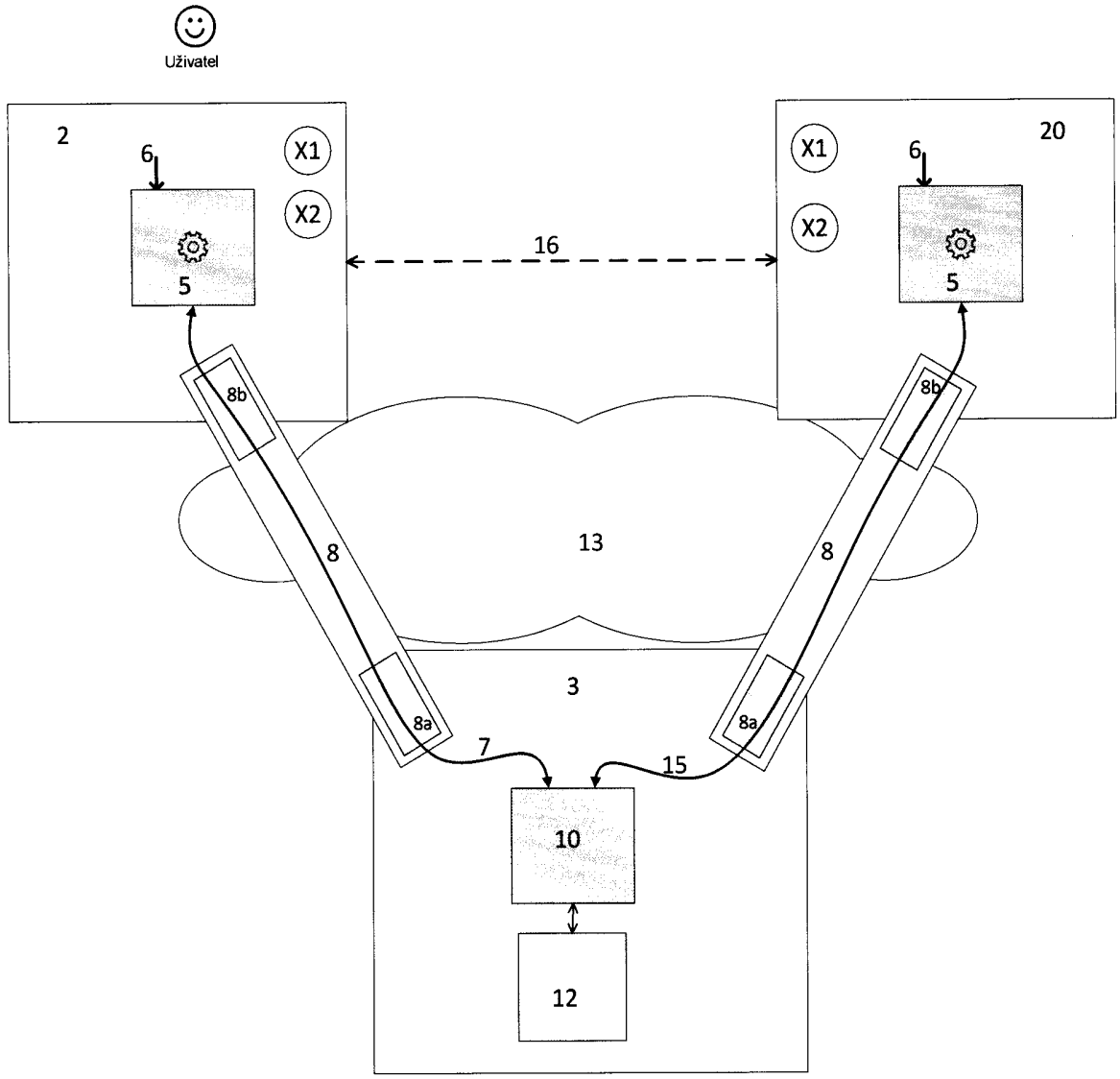


Obr.6

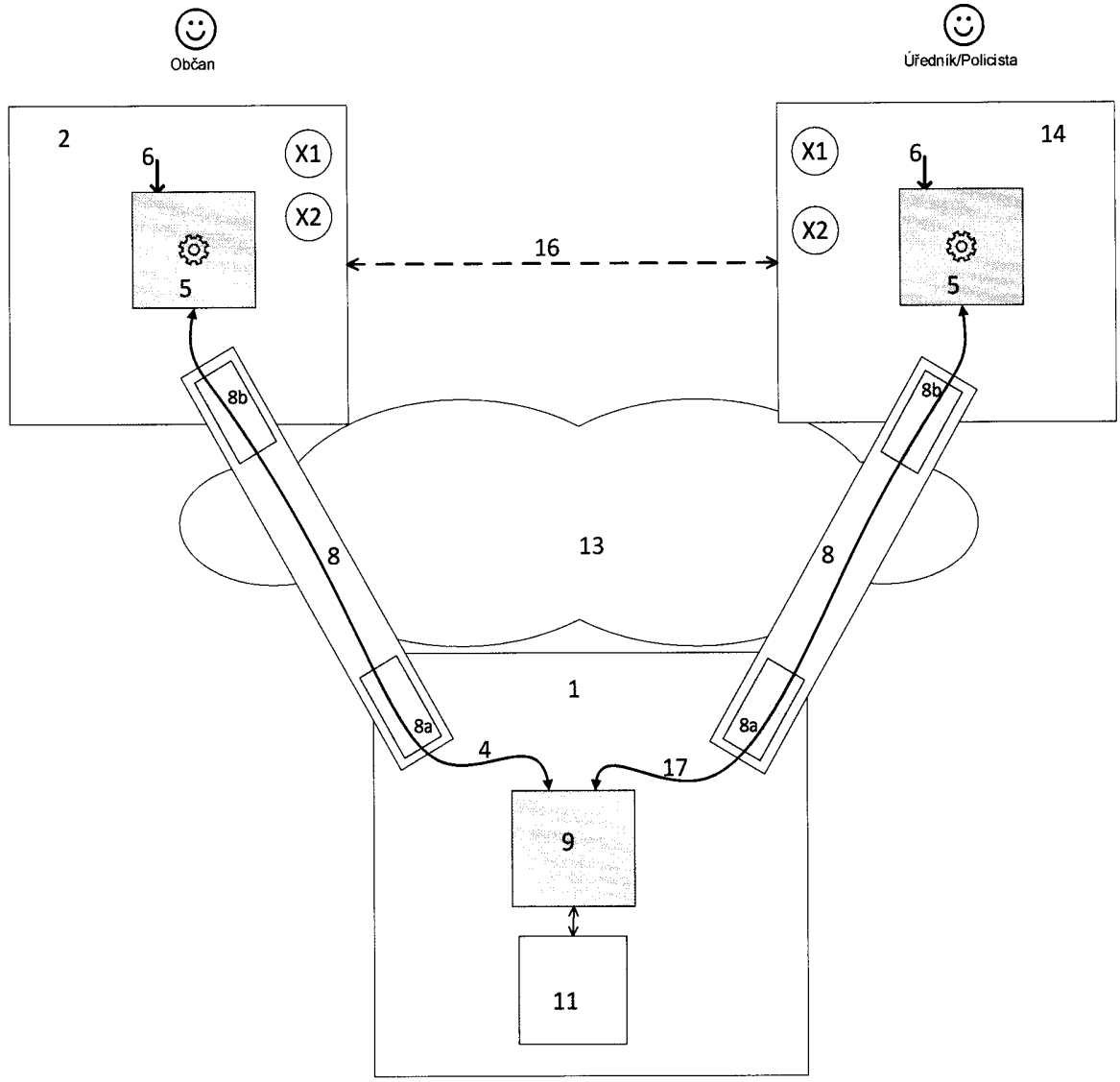


07.07.15

Obr.7



Obr.8


Občan
Úředník/Policista
2
6
X1
X2
5
16
14
X1
X2
6
5
8b
8b
8
8
13
1
8a
8a
4
17
9
11

Obr. 9