Е-УПРАВЉАЊЕ ОРГАНИЗАЦИОНА ТРАНСФОРМАЦИЈА ЕКОНОМСКИ РАЗВОЈ

Бања Лука, 16. и 17. фебруар 2017.

AUSTRIAN DEVELOPMENT COOPERATION

Österreichischer Städtebund

ZENTRUM FÜR VERWALTUNGS FORSCHUNG KDZ

PTPC www.rtrs.tv

Организационо

Семинар се састоји из два дијела

- 16.2. теме из оквира е-Управе
- 17.2. теме из оквира стратегије и развоја

Циљ семинара:

- Преношење знања и искустава експерата који раде у ЕУ
- Академске организације и индустрија
- Актуелне области са акцентом на развојн
- Поријеклом са ових простора

Организационо

Распоред за данас, 16.2.2017.

- 10.30 – 12.00 Технолошке основе е-Управе
- 12.00 – 12.30 Пауза – послужење
- 12.30 – 13.45 Организација услуга е-Управе у Аустрији
- 13.45 – 14.30 Искуства и препоруке са освртом на БиХ

Паузе: по потреби, ~5 минута

Додјела сертификата о учешћу заинтересованим учесницима који су се пријавили само за први дан

Учесници

- Агенција за информационо друштво РС
- Министарство за екон. односе са иностранством
- Агенција за државну управу РС
- Министарство локалне управе и самоуправе
- Секретаријат Владе РС
- Привредна комора РС
- Економски факултет
- Град Бања Лука
- Народна скупштина РС
- Фонд здравственог осигурања РС
- Општине Челинац, Прњавор, Приједор, Градишка
- АПИФ
- Министарство просторног уређења
- Агенција за банкарство РС
- Пореска управа РС
- Републичка агенција за развој МСП
- Градска развојна агенција БЛ
- Гимназија БЛ
- Окружни суд БЛ
- Привреда: Ланако, Мтел, Битлаб, Еуропројект, Сим Импекс, Крајина Осигурање

ТЕХНОЛОШКЕ ОСНОВЕ Е-УПРАВЕ

Бојан Сузић

Бања Лука, 16.2.2017.

AUSTRIAN DEVELOPMENT COOPERATION

Österreichischer Städtebund

ZENTRUM FÜR VERWALTUNGS FORSCHUNG KDZ

PTPC www.rtrs.tv

План

- Терминологија и концепти
- Електронски потпис
- Електронски идентитет
- Аутентикација и Ауторизација
- Управљање идентитетима
- Архитектуре и протоколи идентитета

е-Управа

- Различити термини и обухват
  - е-Управа, е-Управљање, е-Влада, дигитална влада
  - Digital government, e-Government , e-Governance

- Дефиниције
  - .. напори јавних служби усмјерени ка коришћењу ИКТ, и посебно интернета, у сврху унапређивања јавних услуга (OECD)
  - .. орјентисан ка побољшавању ефикасности управе кроз смањивање трошкова комуникације и управљања информацијама, реорганизацију државних агенција и смањење административне подвојености и баријера (ЕУ)

EPRS (2015). eGovernment – Using technology to improve public services and democratic participation
OECD (2014). *Recommendation of the Council on Digital Government Strategies*

е-Управа

- Дефиниције
  - .. стално унапређивање пружања услуга, успостављање учешћа и управљање кроз трансформисање унутрашњих и вањских односа уз помоћ технологије, интернета и нових медија (Гартнер)

- Разлике између (е-)управе и (е-)управљања

е-Управа	е-Управљање
Ел. услуге	Ел. консултација
Ел.и токови	Ел. контрола
Ел. гласање	Ел. ангажовање
Имплементација	Координација
Правила	Циљеви
Одлуке	Процеси

Riley (2004). *E-Governance vs. E-Government. Information for Development*

е-Управа

- Главне карактеристике
  - Трансформација управе
  - Ефикасност и ефективност
  - Једноставност и доступност
  - Транспарентност
  - Корисност

Riley (2004). *E-Governance vs. E-Government. Information for Development*

е-Управа

- Од е-Управе ка дигиталној управи
- Дигитална управа:
  - Употреба дигиталних технологија као дијела модернизационих стратегија ради креирања јавне вриједности. Почива на екосистему који се састоји од учесника из власти, невладиних организација, предузећа, грађанских удружења и појединаца који подржавају производњу и приступ подацима, услугама и садржају кроз интеракције са владом (OECD)

Отвореност и ангажованост

Управљање и координација

Капацитети за подршку

OECD (2014). *Recommendation of the Council on Digital Government Strategies*

е-Управа

- Учесници
  - Грађани
  - Правна лица
  - Јединице управе
  - Запослени
- Орјентисаност ка унутрашњим и вањским интеракцијама
- Врсте процеса:
  - G2C – интеракција између власти и грађана
  - G2B – комуникација између власти и организација
  - G2G – хоризонтална и вертикална комуникација унутар институција
  - G2E – пружање сервиса запосленим у институцијама

Модел зрелости е-Управе

	Трансакција	Процес се у потпуности електронски обавља Интегрисани кораци без прекида Повезане и интегрисане базе података
Интеракција	Обострана интеракција	Електронски формулари Структуирани подаци
	Једнострана интеракција	Преузимање формулара за покретање процедуре Интерактивне базе знања
	Информација	Служење статичких информација Базичне информације на веб сајту

е-Управа 2.0

Персонализација	Аутоматизовано попуњавање формулара Контекстуално прилагођен
Трансакција	Процес се у потпуности електронски обавља Интегрисани кораци без прекида Повезане и интегрисане базе података
Обострана интеракција	Електронски формулари Структуирани подаци
Једнострана интеракција	Преузимање формулара за покретање процедуре Интерактивне базе знања
Информација	Служење статичких информација Базичне информације на веб сајту

е-Управа

ЕУ акциони план 2016-2020 – убрзавање дигитализације

Кључни принципи:

- Дигитална влада у старту
  Преференција дигиталних сервиса и једне приступне тачке
- Начело једне интеракције
  Информација се обезбјеђује само једном, без додатних оптерећења
- Инклузивност и приступачност
- Отвореност и транспарентност
  Интерна размјена информација укључујући грађане у надледање процеса
- Међуграничне интеракције као стандард
- Интероперабилност у старту
  Интеракције међу државама и унутар организација без препрека
- Повјерење и сигурност

EC (2016). Communication 179 – EU eGovernment Action Plan 2016-2020

Темељи услуга е-Управе

е-Потпис

Успоставља интегритет, аутентичност и непорецивост интеракција.
Значајан чинилац за е-Докумената и е-ИД.

е-Документ

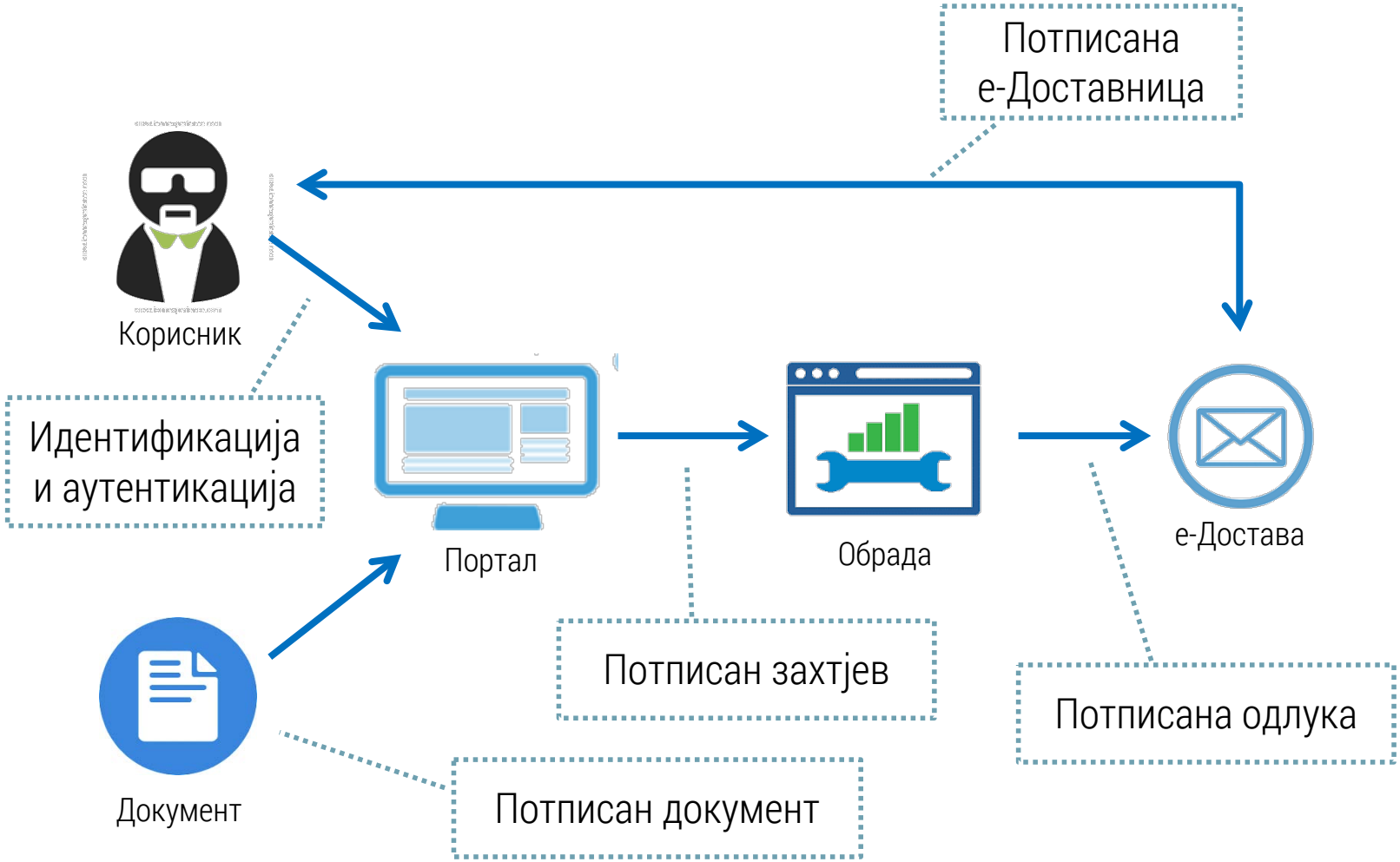
Електронски, структуирани документи који се могу размјењивати у интеракцијама између актера

е-Идентификација

Омогућава јединствену идентификацију и сигурну аутентификацију у електронским процесима

е-Потпис

Употреба потписа у типичном процесу и интеракцијама



Правни оквир е-Потписа

Иницијални правни оквир одређен ЕУ директивом 1999/93/ЕС

Од 2016. године мјеродавна је eIDAS уредба 910/2014

Врсте потписа:

- Електронски потпис
- Напредни електронски потпис
- Квалификовани електронски потпис

Електронски потпис – eIDAS чл. 3 (10):

- ‘electronic signature’ means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;

Directive 1999/93/EC ... on a Community framework for electronic signatures
Regulation No 910/2014 ... on electronic identification and trust services for electronic transactions in the internal market...

Правни оквир е-Потписа

Напредни електронски потпис – eIDAS чл. 26:

- An advanced electronic signature shall meet the following requirements:
  (a) it is uniquely linked to the signatory;
  (b) it is capable of identifying the signatory;
  (c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
  (d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

Подаци за креирање и провјеру потписа су једнозначни и придружени само једном субјекту

Одговара приватном и јавном криптографском кључу

Правни оквир е-Потписа

Напредни електронски потпис – eIDAS чл. 26:

- An advanced electronic signature shall meet the following requirements:
  (a) it is uniquely linked to the signatory;
  (b) it is capable of identifying the signatory;
  (c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
  (d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

Потпис се може креирати и провјерити само уз помоћ одговарајућег приватног кључа и провјерити само са упареним јавним кључем

Практично немогуће креирати исти пар кључева више пута

Практично немогуће извести приватни кључ из јавног кључа

Правни оквир е-Потписа

Напредни електронски потпис – eIDAS чл. 26:

- An advanced electronic signature shall meet the following requirements:
  (a) it is uniquely linked to the signatory;
  (b) it is capable of identifying the signatory;
  (c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
  (d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

Потпис се може креирати само од стране ауторизоване особе

Контрола могућа кроз аутентификацију (фактори)

Правни оквир е-Потписа

Напредни електронски потпис – eIDAS чл. 26:

- An advanced electronic signature shall meet the following requirements:
  (a) it is uniquely linked to the signatory;
  (b) it is capable of identifying the signatory;
  (c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
  (d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

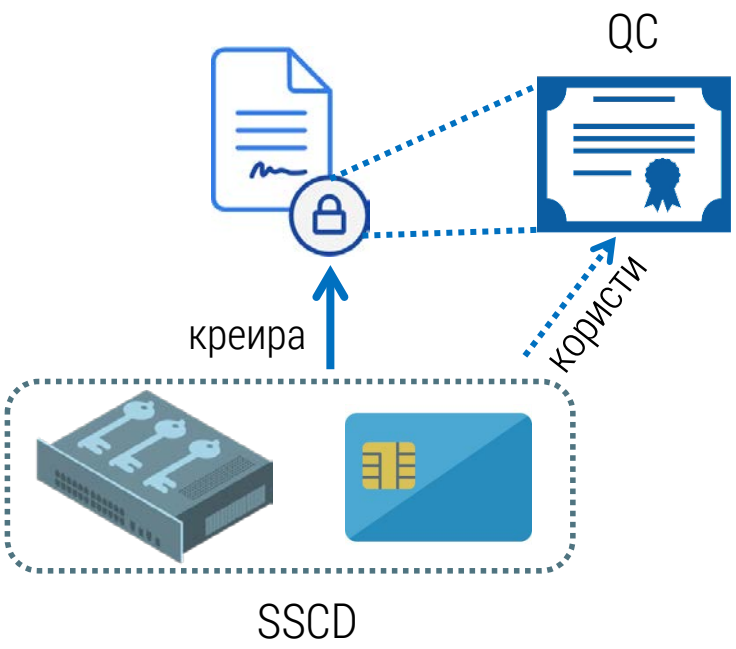
Практично немогуће да:

- различити подаци дају исту хеш вриједност
- било који податак даје исту хеш вриједност

Правни оквир е-Потписа

Квалификовани електронски потпис – eIDAS чл. 3 (12):

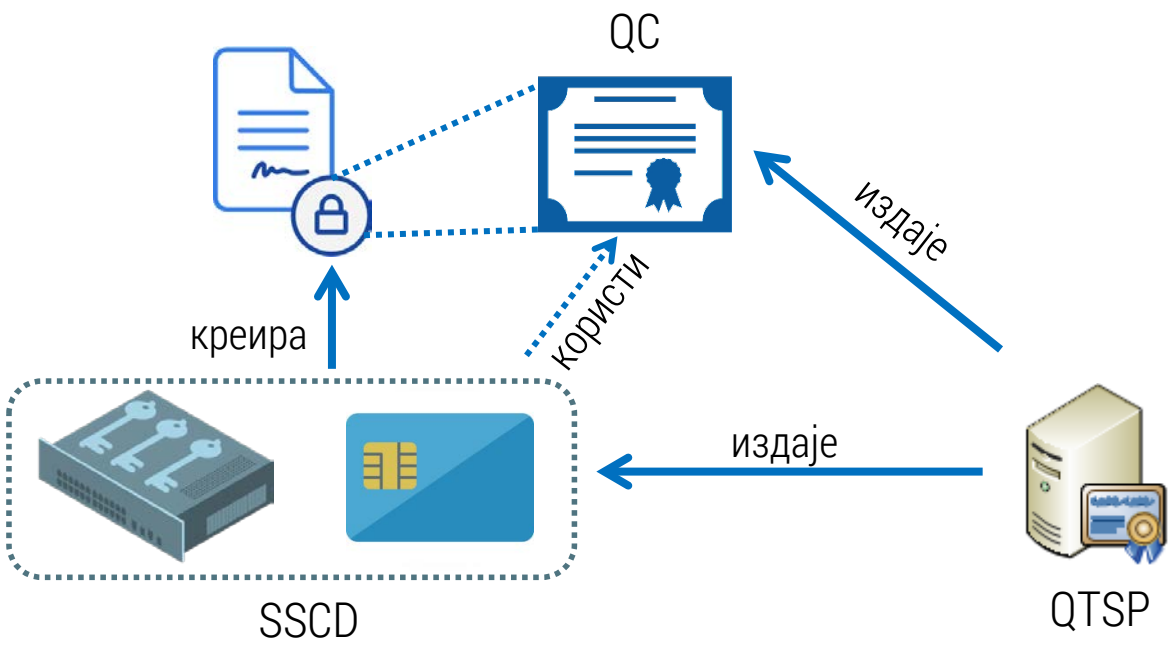
- напредан електронски потпис који је израђен помоћу квалификованих средстава за израду електронског потписа (SSCD), и заснива се на квалификованом сертификату за електронске потписе (QC)



Правни оквир е-Потписа

Квалификовани сертификат (QC):

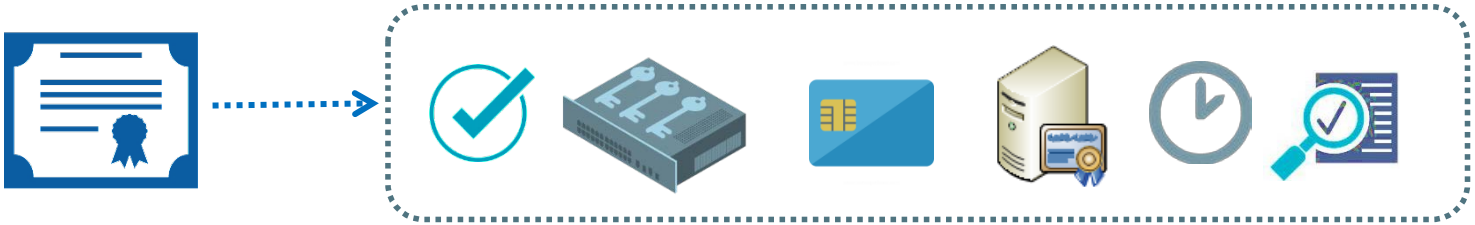
- издат од стране квалификованог добављача услуга повјерења (QTSP)
- одговара захтјевима из уредбе



Правни оквир е-Потписа

Захтјеви за квалификовани сертификат – eIDAS прилог 1:

- назнака да је сертификат квалификован
- податке о квалификованом добављачу услуга повјерења
- име или псеудоним потписника
- подаци за провјеру потписа и сертификата
- податке о раздобљу важења сертификата
- потпис добављача који издаје сертификат
- индикација ако је потпис настао путем квалификованог уређаја за потписе

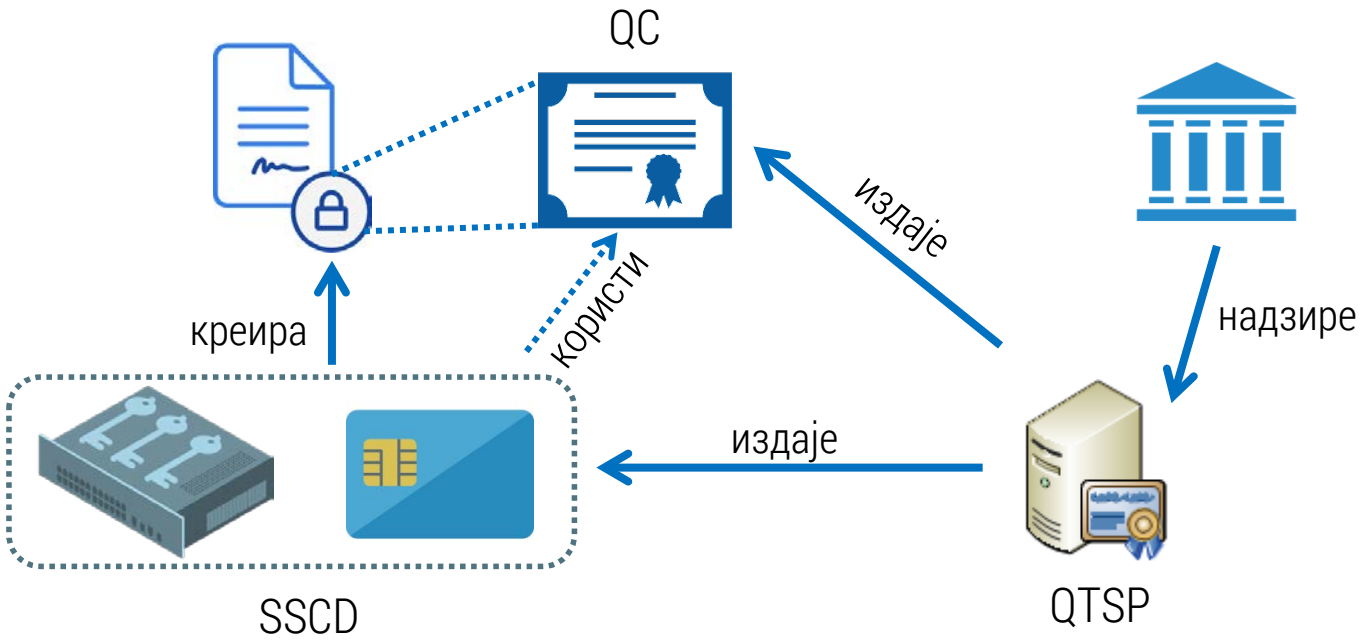


Regulation No 910/2014 ... on electronic identification and trust services for electronic transactions in the internal market...

Правни оквир е-Потписа

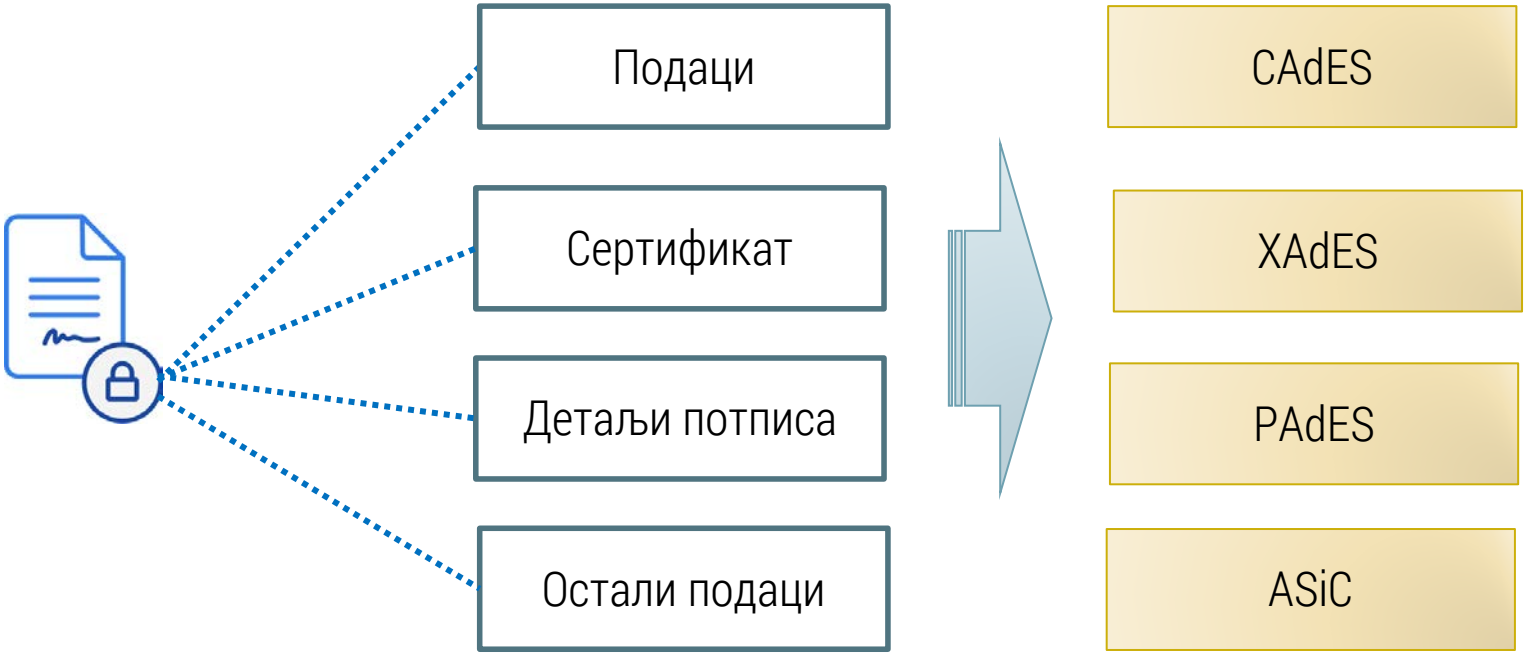
Услуге повјерења чине:

- креирање, верификацију и валидацију
- односе се на електронске потписе, печате, временске жигове, препоручену електронску доставу и сертификате повезане са тим услугама



Формати е-Потписа

Подаци потребни за провјеру потписа



AdES – Advanced Signature Formats (CMS, XML, PDF)

Формати е-Потписа

XAdES – XML Advanced Electronic Signatures

CAdES – CMS Advanced Electronic Signatures

PAdES – PDF Advanced Electronic Signatures

Профили:

BES – Basic Electronic Signature

Основни формат, задовољава захтјеве из директиве

EPES – Explicit Policy-based Electronic Signature

Одређивање политике за провјеру потписа

T – Timestamp

Додатно садржи временски жиг

Формати е-Потписа

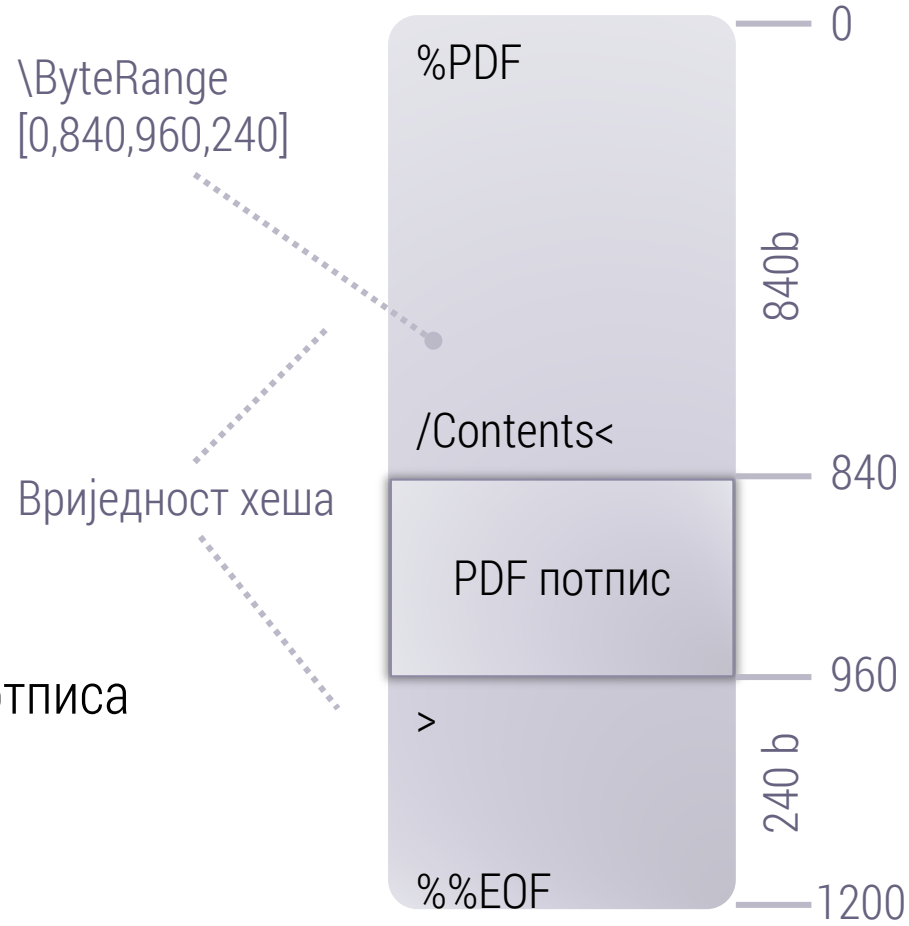
PAdES – примјер уграђивања потписа

Потпис је укључен у документ

Потпис садржи:

- Сертификат
- Сажетак
- Временски код

ByteRange се користи код провјере потписа



Формати е-Потписа

Провјера потписа

Укључује два корака:

- Криптографска провјера
- Провјера сертификата

Криптографска провјера:

- Обрачун и поређење вриједности сажетка (hash value)
  - Показује да документ није накнадно мијењан
- Провјера вриједности потписа
  - гарантује аутентичност потписа
  - успоставља везу са потписником

Формати е-Потписа

Провјера сертификата

Успостављање ланца сертификата

- Од потписника до коријенског сертификата (root)

За сваки сертификат у ланцу:

- Провјерити период важења
- Провјерити опозив користећи OCSP или CRL

Провјерити да ли је сертификат уврштен у одговарајући профил повјерења (trust profile)

Провјерити сертификат потписника

Статус квалификованог сертификата (QC)

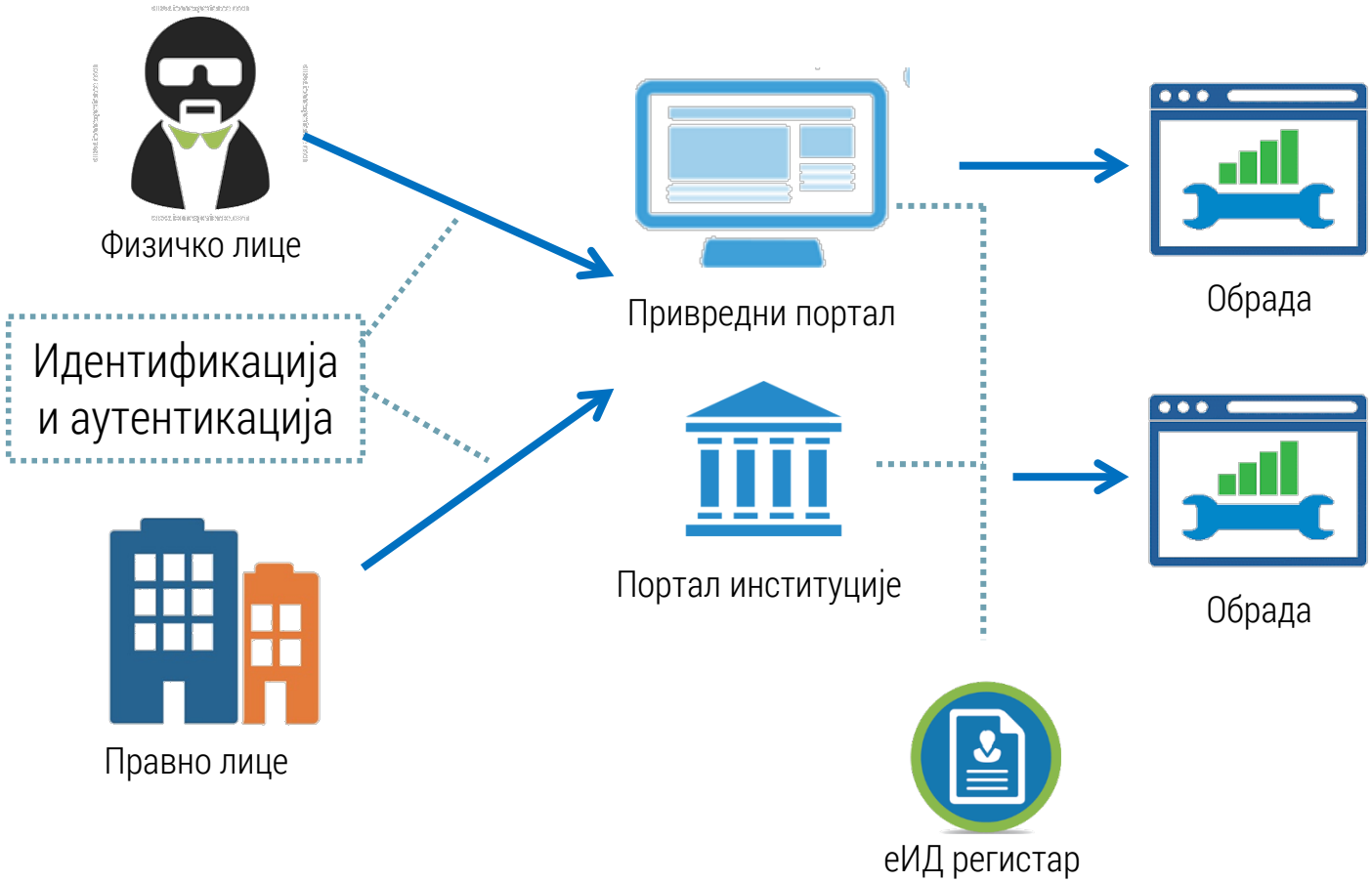
Статус уређеја за креирање потписа (SSCD)

е-Идентификација

Омогућава јединствену идентификацију и сигурну аутентификацију у електронским процесима

е-Идентификација

Идентификација грађана и правних субјеката



Идентитет

Шта је идентитет?

Карактеристика која одређује особу или ствар.

Одређујућа карактеристика или личност појединца.

Релативно стабилно разумјевање и очекивање о себи, прилагођено улози.

Карактеристике које чине особу различитом (јединствене или опште)

Име, пол, боја очију, висина

Припадност организацији, осјећај припадности, вјеровања

Cambridge Dictionary
Oxford Dictionary
Wendt (1994). Collective Identity Formation and the International State.

Дигитални идентитет

Дигитална репрезентација информације о појединцу или организацији.

Скуп сталних или готово сталних временских атрибута придружених ентитету.

Репрезентација људског идентитета која се користи у дистрибуираној мрежној интеракцији са другим људима или машинама.

Атрибути и особине личности, али доступне у дигиталној форми

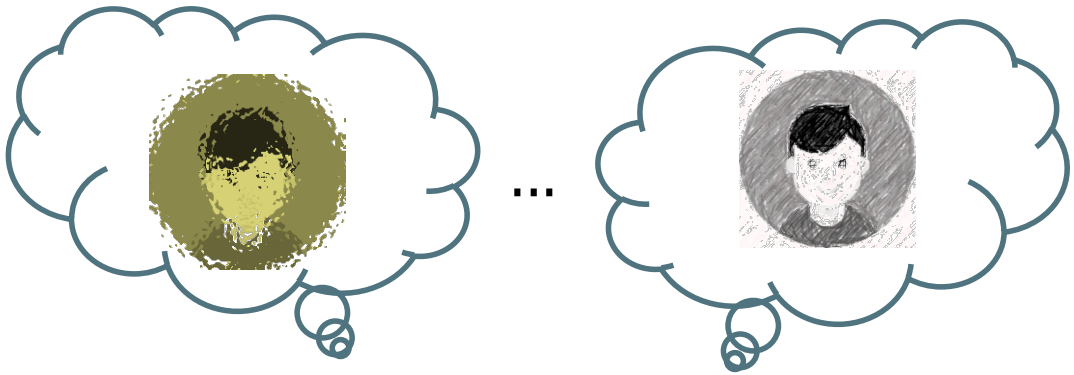
- Име, датум рођења, корисничко име, е-пошта

Може да се придружи и другим субјектима:

- Предузећа, организације, рачунарски системи

Bertino & Takahashi (2011). Identity management: Concepts, Technologies, and Systems.
Camp (2004). Digital Identity.
DigitalID World Magazine.

Дигитални идентитет



Дигитални идентитет

односи се на

односи се на

Идентификатор

представља

Особа

marko@markovic.biz

Gini-SA (2011). A User-centric Framework of Identity Management Services

Дигитални идентитет

По ITU-T Y.2720 препорукама идентитет је:

- Информација о ентитету која је довољна да се ентитет идентификује у конкретном контексту (окружењу)

Дигитални идентитет

Идентификатор

marko@markovic.biz
http://id.state/person#marko
A1234882

Акредитив (Credential)

Атрибут

International Telecomunication Union (2010). Recommendation ITU-T Y.2720.
Bertino & Takahashi (2011). Identity management: Concepts, Technologies, and Systems..

Дигитални идентитет

Врсте идентитета:

- Псеудонимни – страна од повјерења одваја диг. идентитет од стварне особе
  Повезивање стварног и псеудо-идентитета може да изврши само та страна
- Анонимни – комплетно се одваја диг. идентитет од стварне особе

Важење идентитета:

- Локално окружење
  Примјер: локални рачунар
- Глобално окружење
  Примјер: пасош
- Федерализовано окружење
  Примјер: Једнострука пријава (Single Sign-On)
- Преко посредника
  Примјер: превођење дјелимичног на псеудо-идентитет (приватност)

Ел. идентитет - еИД

Гарантује јединствен идентитет лица (физичко или правно)

- Представља базу за странке укључене у ел. трансакцији

Особине које треба да обезбједи:

- Универзалност покривања
- Јединственост
- Сталност
- Ексклузивност
- Тачност

Код осјетљивих примјена:

- Идентификација
- Потпис
- Аутентификација

Идентификација

Придуживање личног идентификатора појединцу.

Придуживање атрибута лицу

- „Марко Марковић“ идентификује особу са именом Марко Марковић

Јединственост:

- Ако у оквиру контекста примјене постоји више лица са атрибутом потребно је обезбједити додатне атрибуте који сужавају избор
- Нпр: датум рођења, ЈМБГ, адреса, име оца

Традиционално:

- Пасош, возачка дозвола, лична карта

Онлајн: еИД

Идентификација

Средства идентификације

Начин	Опис	Примјер
Изглед	Како особа изгледа	Боја очију, фотографија
Понашање	Како особа ступа у контакт са околином	Глас, историја разговора, банковне трансакције
Имена	Називи особе у контакту са другим људима	Презиме, надимак, име из националног регистра
Кодови	Ознака особе у организацији	ЈМБГ, број индекса, личне карте
Токени	Шта особа посједује	Возачка дозвола, паметна картица, мобилни телефон
Биометрија	Шта је особа	Отисак прста, ретине, ДНК

Аутентикација

Аутентикација је доказ посједовања атрибута.

Аутентикација идентитета је доказивање асоцијације између особе и идентификатора.

Процес провјере тврдње о субјекту о посједовању атрибута.

Традиционални приступ:

- Провјера идентитета путем прегледа личне карте

Онлајн:

- Провјера идентитета употребом лозинке или е-потписа

Clarke (1994). Human identification in information systems: Management challenges and public policy issues.
Gini-SA (2011). A User-centric Framework of Identity Management Services

Механизми аутентикације

Начин	Опис
Знати	Познавање неке информације Лозинка, ПИН, одговор на питање
Посједовати	Посједовање средства за доказ идентитета Лична карта, пасош, паметна картица, приватни кључ
Бити	Лична карактеристика Отисак прста, скенирање ретине
Радити нешто	Образац понашања, глас

Аутентикација у више корака (фактора)

- Комбиновање више механизама ради повећања сигурности и прецизности

Примјери за два фактора:

- Паметна картица и ПИН-код
- Мобилни телефон и лозинка

Ауторизација

Одлука да се дозволи извршење неке операције на основу идентификатора или атрибута.

Процес придруживања дозвола у систему дигиталном идентитету.

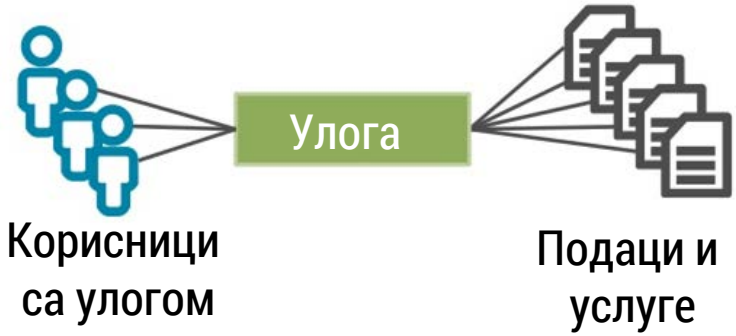
Обично се извршава након аутентикације

Односи се на придруживање приступних права ентитету

- Читање или писање података, приступ документима
- Отварање налога, извршавање пословне активности

Модели контроле приступа:

- MAC – Mandatory Access Control
- RBAC – Role-based Access Control
- ABAC – Attribute-based Access Control
- OrBAC – Organization-based Access Control



Samarati (2010). Access control: Policies, Models and Mechanisms.

Сумирано

Идентитет

- „Марко Марковић“

Идентификација

- „Ја сам Марко Марковић“

Аутентикација

- „Моја лична карта доказује да сам ја Марко Марковић“

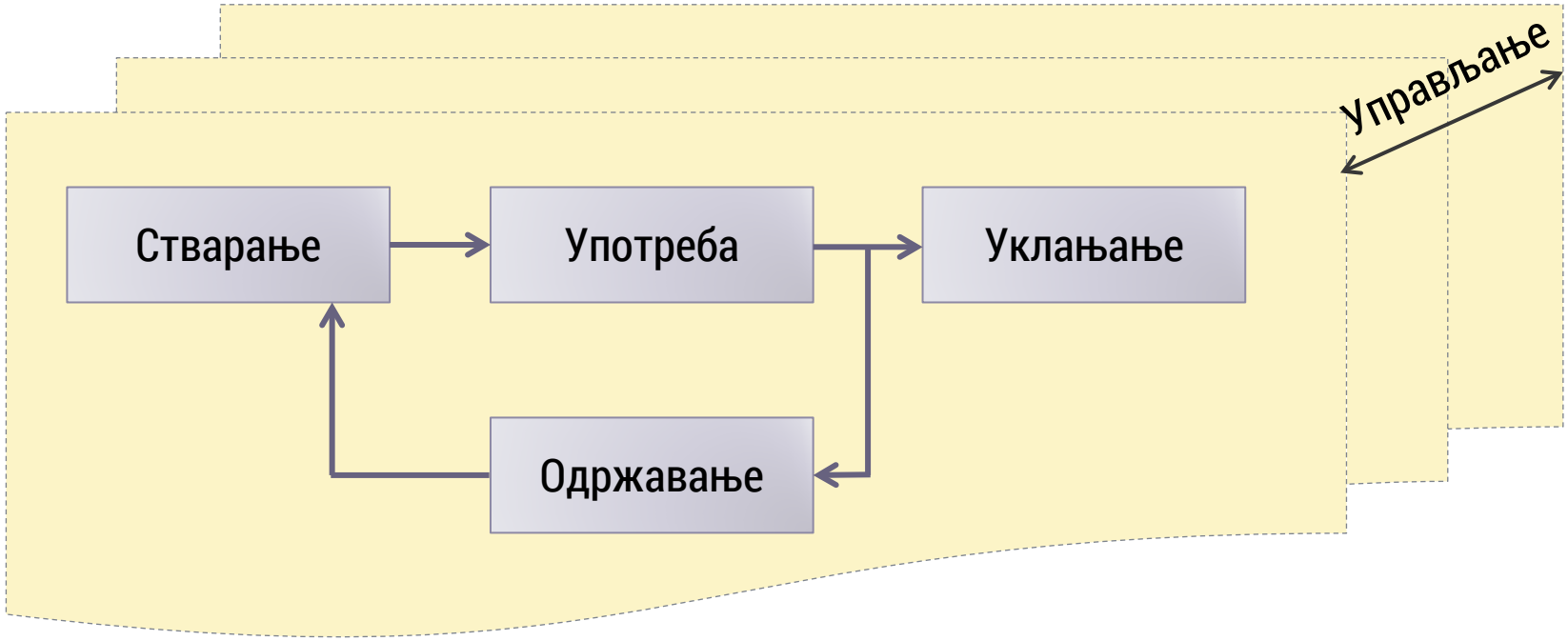
Ауторизација

- „Марко Марковић може да приступи сервису А због тога што је запослен у организацији Б и посједује улогу Ц“

Управљање идентитетима

Identity Management (IdM) – Identity and Access Management (IAM)

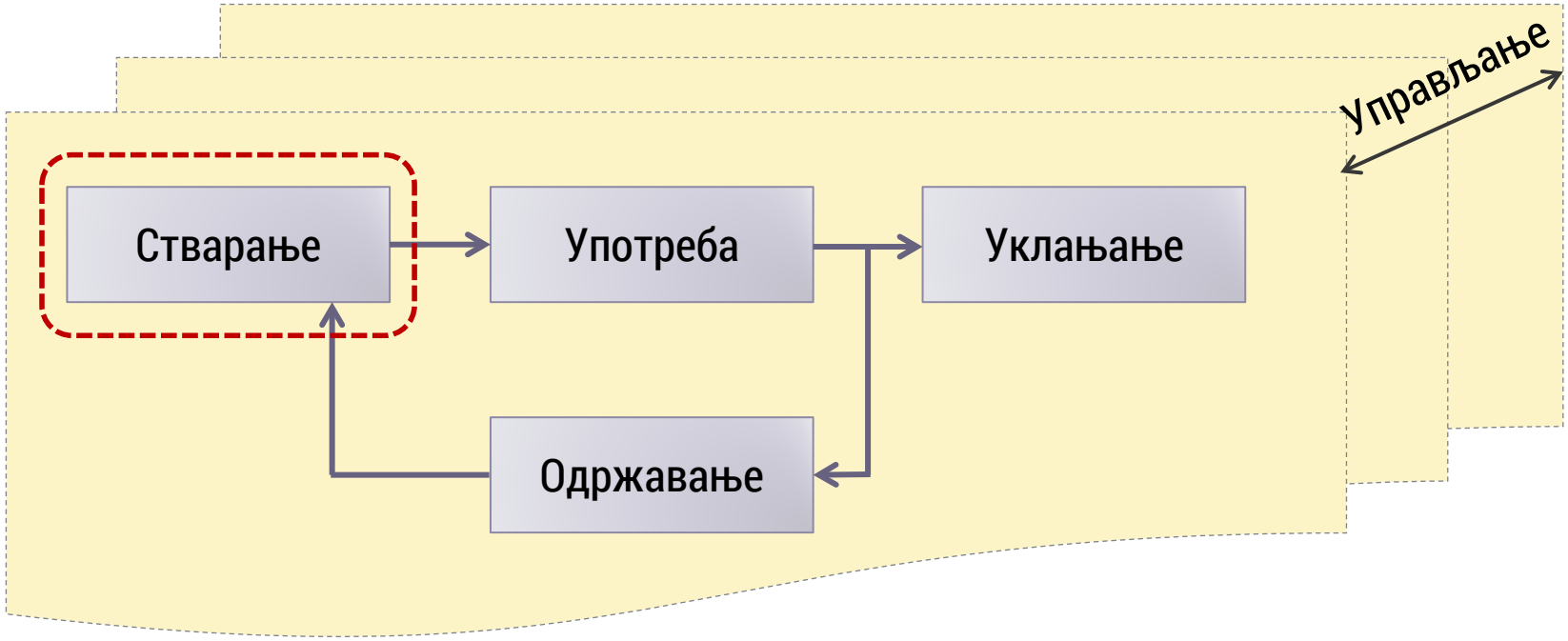
- Управљање дигиталним идентитетима путем процеса, технологија и политика који одређују њихово коришћење и животни циклус



Управљање идентитетима

Стварање идентитета

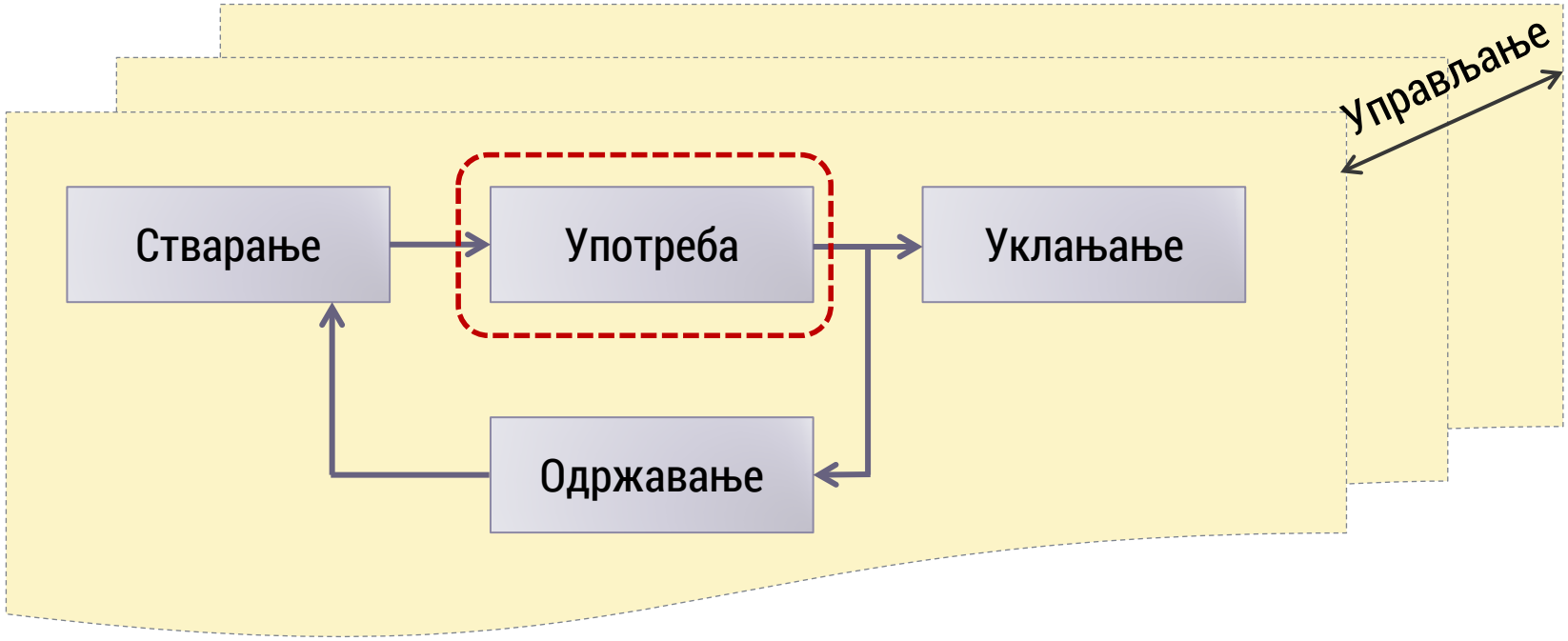
- Успостављање записа о дигиталном идентитету
- Може да задржи више атрибута (декларисани и/или провјерени)
- Издавање акредитива (credential)



Управљање идентитетима

Употреба идентитета

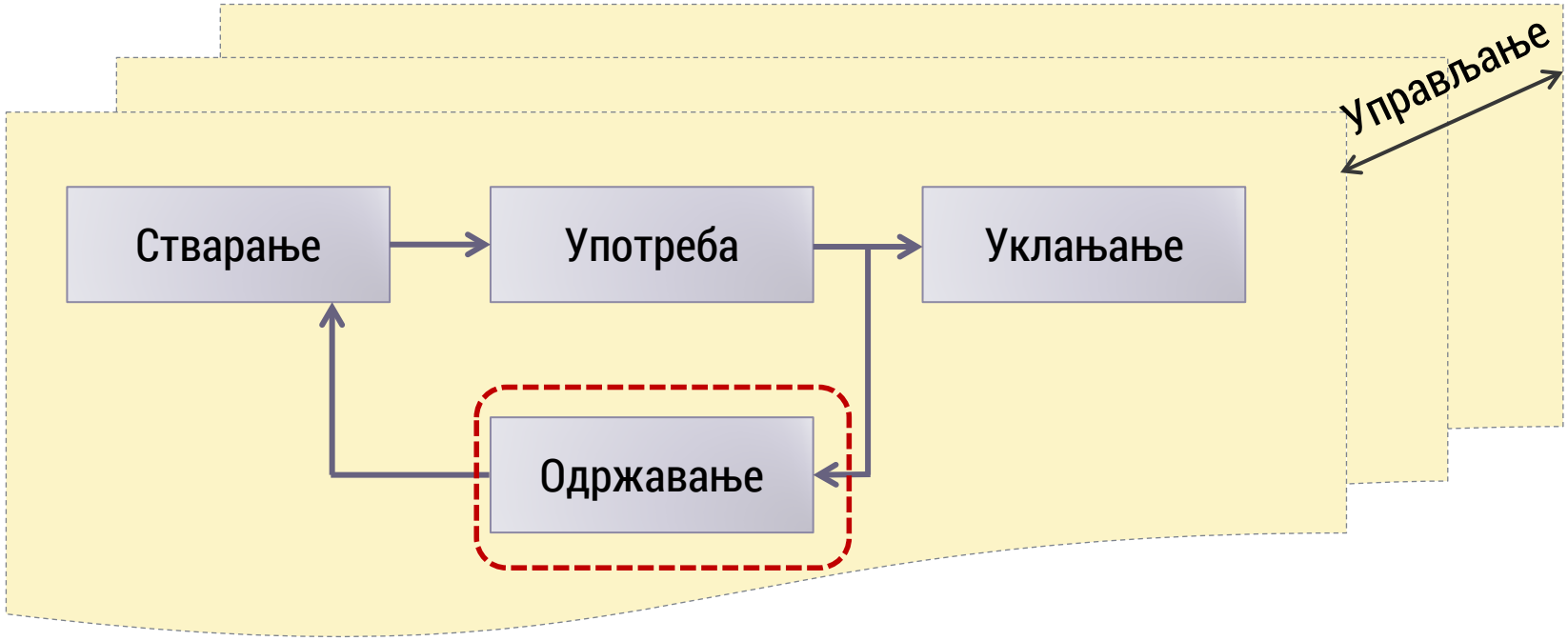
- Пријава на сервисе
- Ауторизација и аутентикација
- Једнострука пријава на више сервиса – Single Sign-On (SSO)



Управљање идентитетима

Одржавање

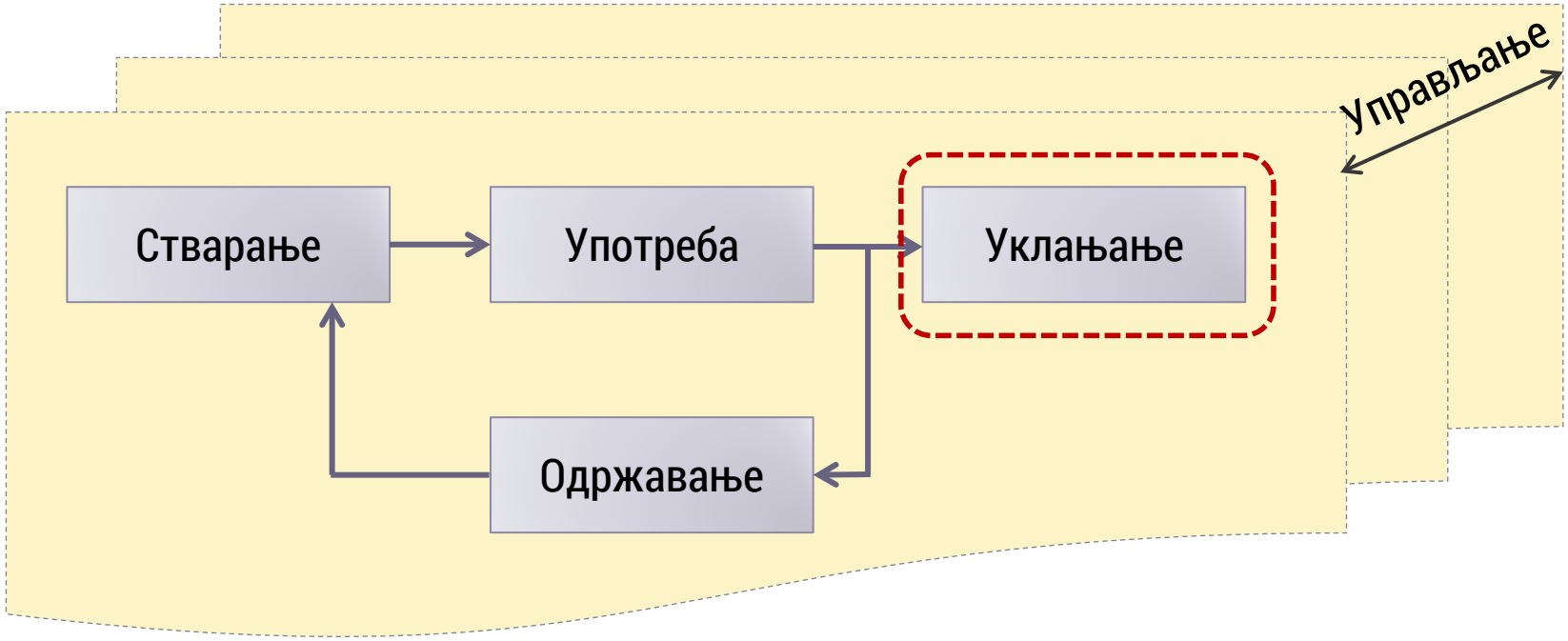
- Додавање или промјена атрибута (нпр. ажурирање адресе)
- Истек атрибута (нпр. важење сертификата)
- Идентификатори остају константни



Управљање идентитетима

Уклањање

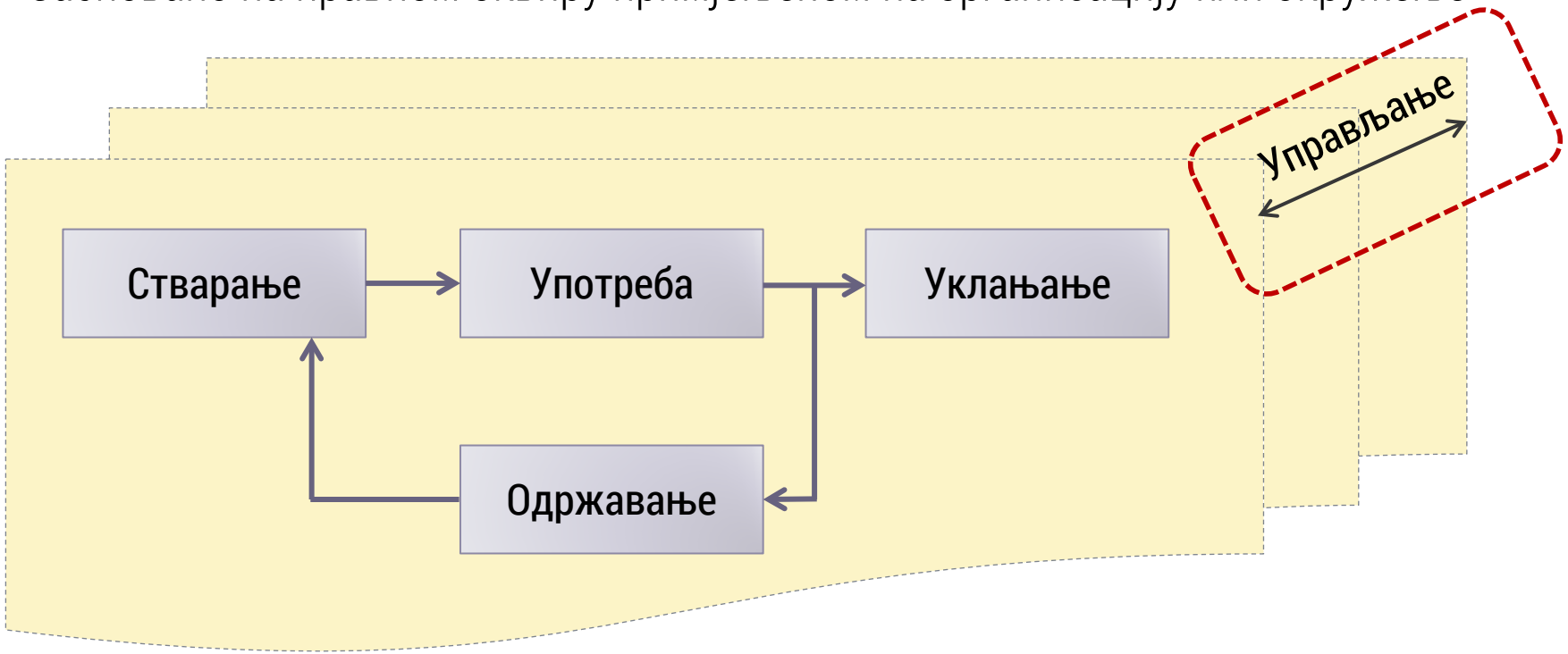
- Ручно уклањање
- Истек (expiry)
- Опозив (revocation)



Управљање идентитетима

Управљање одређује смјернице:

- Код процеса стварања, употребе, уклањања, одржавања
- Код праћења и евидентирања активности
- Код аутентификације (ниво и јачина), ауторизације (модели и услови)
- Засновано на правном оквиру примјењеном на организацију или окружење



Нивои осигурања

Осигурање (Levels of Assurance) представља квантитативну мјеру поузданости процеса који воде до и укључују активност аутентикације

Више приступа:

- ISO/EIC 29115, NIST SP 800-63 – 4 нивоа
- eIDAS – 3 нивоа

Нивои осигурања

Осигурање (Levels of Assurance) представља квантитативну мјеру поузданости процеса који воде до и укључују активност аутентикације

ISO/EIC 29115, NIST SP 800-63 – 4 нивоа

Технички оквир

Фаза уписа	Пријава, Регистрација, провјера идентитета, чување записа
Управљање акредитивима	Креирање, обрада, повезивање, издавање, активација, складиштење, суспензија...
Аутентикација	Аутентикација Чување записа

Управљање и организација

Успостављање услуге, правна и уговорна усклађеност, финансијска обезбјеђења, ИТ сигурност и ревизија, спољне компоненте, оперативна инфраструктура...

ITU-T Recommendation X.1254 | ISO/IEC DIS 29115 - Entity authentication assurance framework

Нивои осигурања

Осигурање (Levels of Assurance) представља квантитативну мјеру поузданости процеса који воде до и укључују активност аутентикације

eIDAS – 3 нивоа

Технички оквир

Упис	Пријава и регистрација; провјера идентитета (физичка и правна лица); повезивање средстава идентификације;
Управљање средствима идентификације	Карактеристике и дизајн; издавање, испорука и активација; суспензија, опозив и реактивациа; обнова и промјена
Аутентикација	Аутентикациони механизам Чување записа

Управљање и организација

Општа обезбјеђења; објављене информације; управљање ИТ сигурношћу; чување записа; опрема и запослени; технички услови; усклађеност и ревизија

Commission Implementing Regulation (EU) 2015/1502

Нивои осигурања

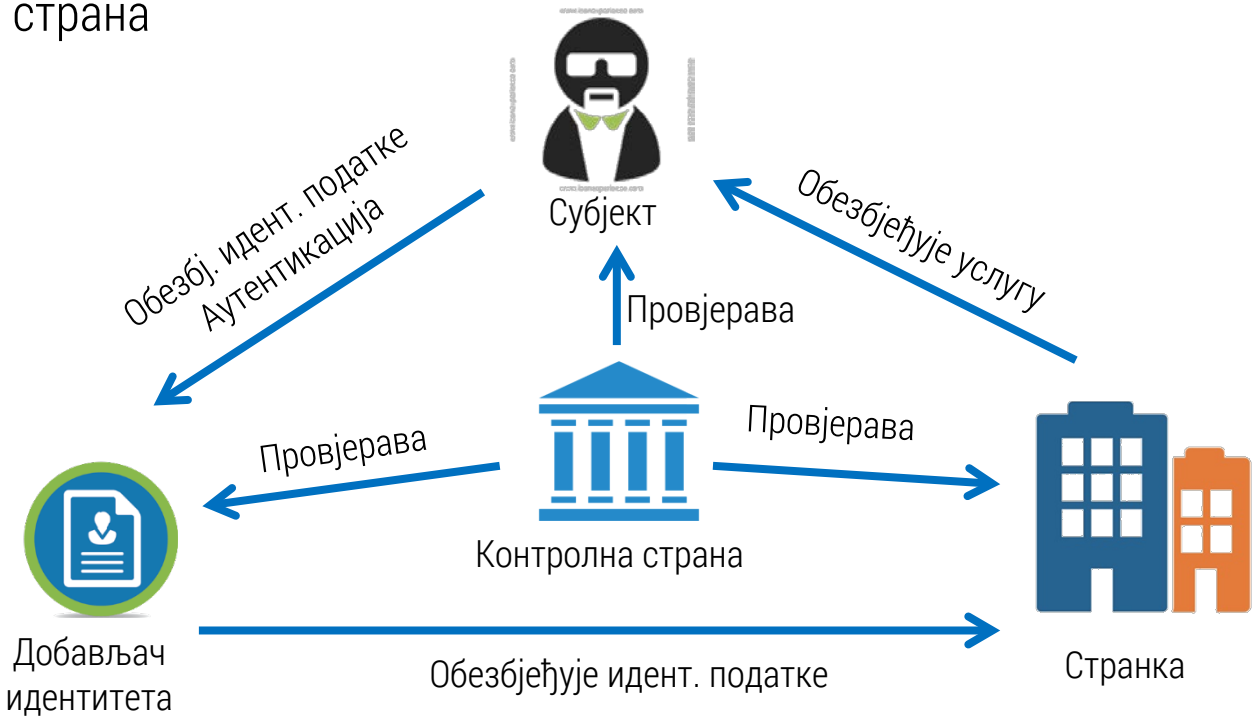
Поређење различитих стандарда и нивоа

eIDAS	STORK QAA	ISO 29115	NIST	Опис - сумирано
	Ниво 1	LoA 1	Ниво 1	Корисничко име и лозинка Нпр Facebook ID
Низак	Ниво 2	LoA 2	Ниво 2	Име и јака лозинка послани на стално пребивалиште
Значајан	Ниво 3	LoA 3	Ниво 3	OTP на регистрован телефон или лично издан софт. сертификат
Висок	Ниво 4	LoA 4	Ниво 4	Хардв. сертификат издат путем личне контроле субјекта од стране акредитоване институције

Архитектуре идентитета

Учесници у процесу:

- Субјект
- Добављач идентитета (Identity Provider – IdP)
- Странка (Relying Party / Service Provider)
- Контролна страна

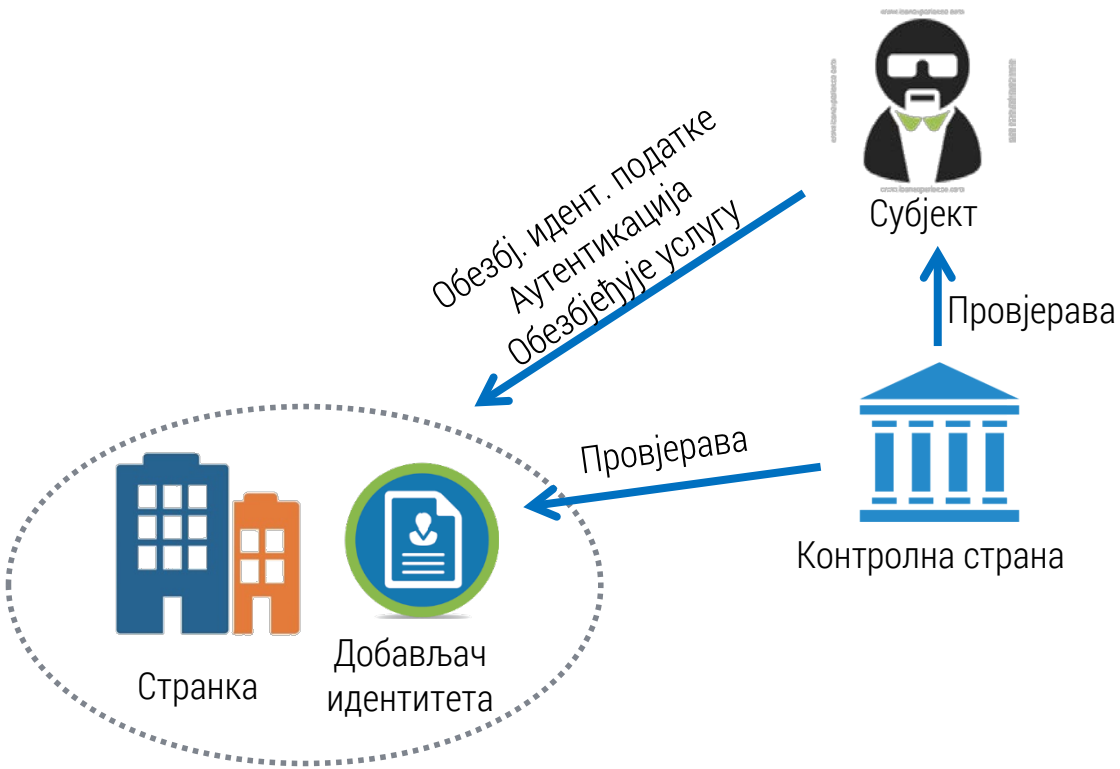


Bertino & Takahashi (2011). Identity management: Concepts, Technologies, and Systems..

Архитектуре идентитета

Изоловани модел

- Добављач идентитета и странка спрегнути (IdP-SP)

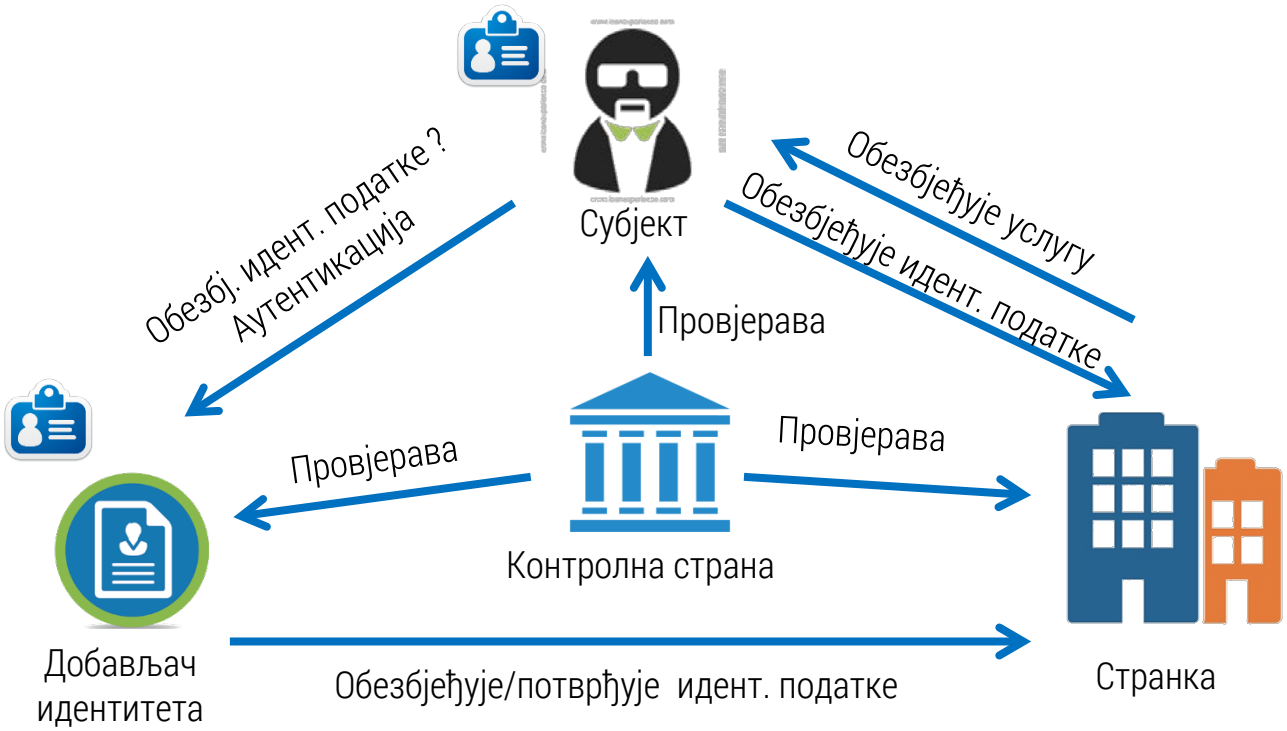


Zwattendorfer et al. (2014). An Overview of Cloud Identity Management-Models.

Архитектуре идентитета

Централизовани и корисничко-центрирани модел

- Добављач идентитета или корисник имају потпуну контролу над складиштењем и преношењем идентификационих података
- Facebook/Google насупрот паметне картице

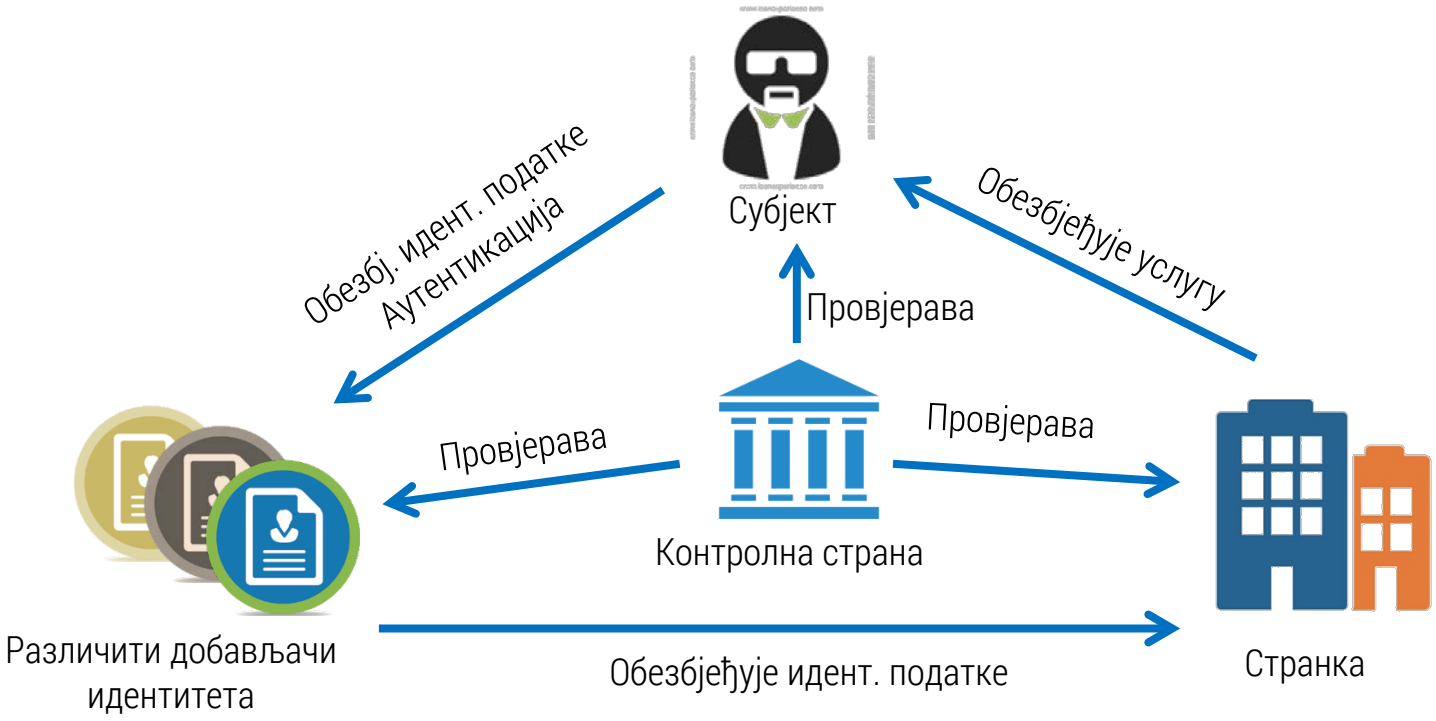


Zwattendorfer et al. (2014). An Overview of Cloud Identity Management-Models.

Архитектуре идентитета

Федерализовани модел:

- Више добављача идентитета подсједују и размјењују идентификационе податке
- Релација повјерења и процеси размјене успостављени између добављача
- Постоји заједнички именитељ идентификатора

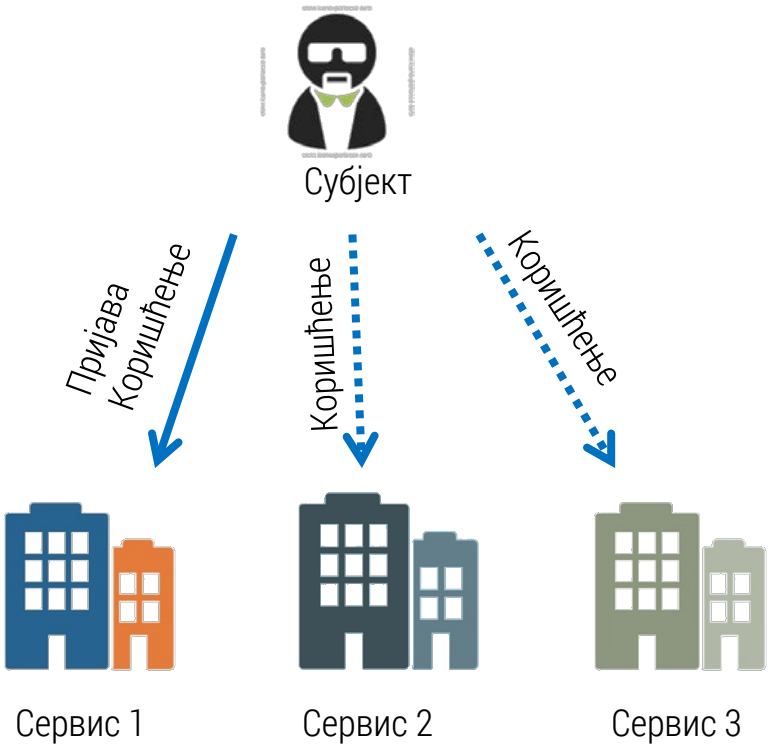


Zwattendorfer et al. (2014). An Overview of Cloud Identity Management-Models.

Једнострука пријава

Једнострука пријава и одјава (Single Sign-On, Single Logout)

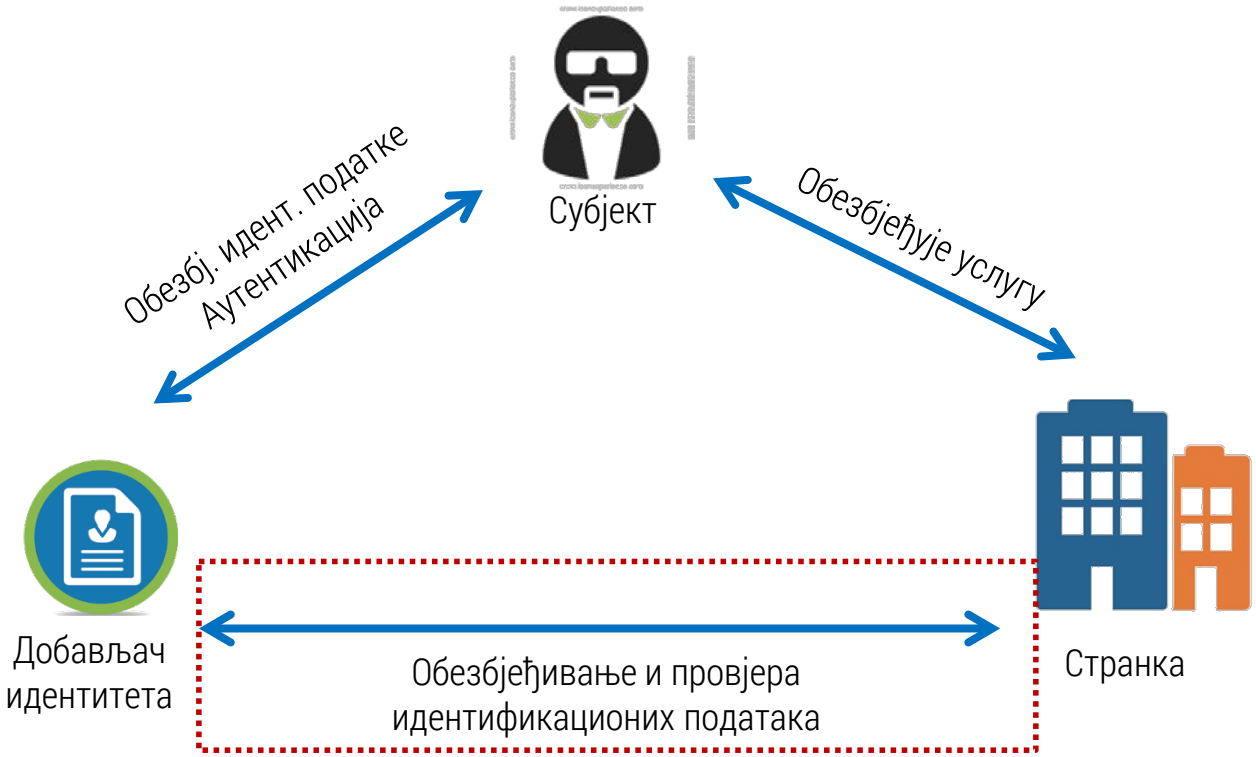
- Могућност за корисника да се аутентификује једном и да након тога исту пријаву користи за приступ другим сервисима без поновне аутентикације
- Кумулативно одјављивање са више сервиса



Протоколи за идентитете

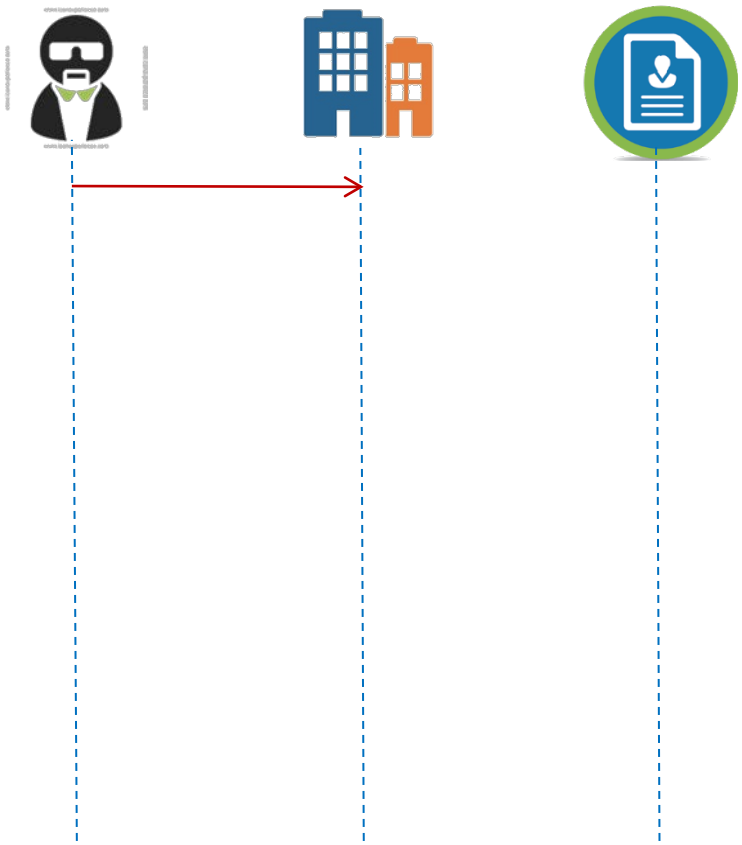
Протоколи одређују начин и правила комуникације између актера

- Размјена информација између добављача идентитета и сервиса
- Једнострука пријава и одјава (SSO/SLO)



Протоколи за идентитете

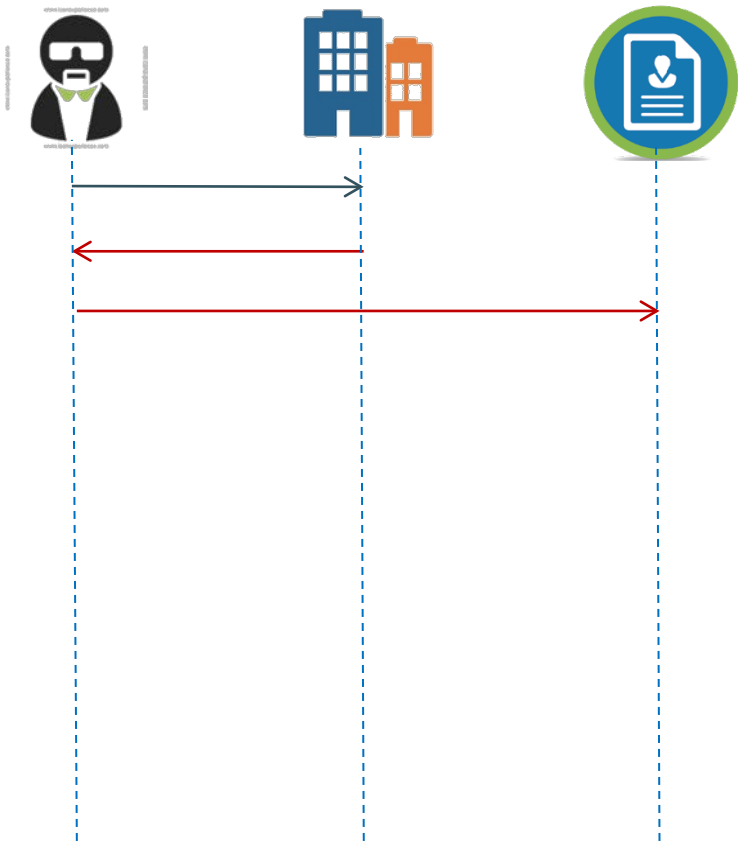
Типичан процес пријаве



- Корисник приступа заштићеном ресурсу

Протоколи за идентитете

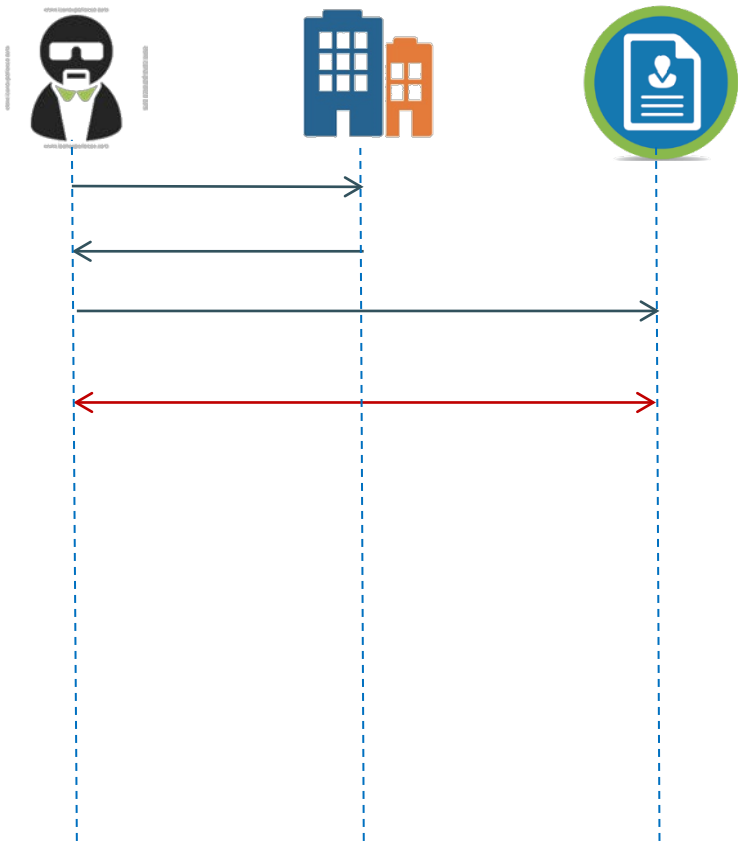
Типичан процес пријаве



- Корисник приступа заштићеном ресурсу
- Сервис преусмјерава корисника ка добављачу идентитета са захтјевом да се пријави (захтјев за аутентикацију)

Протоколи за идентитете

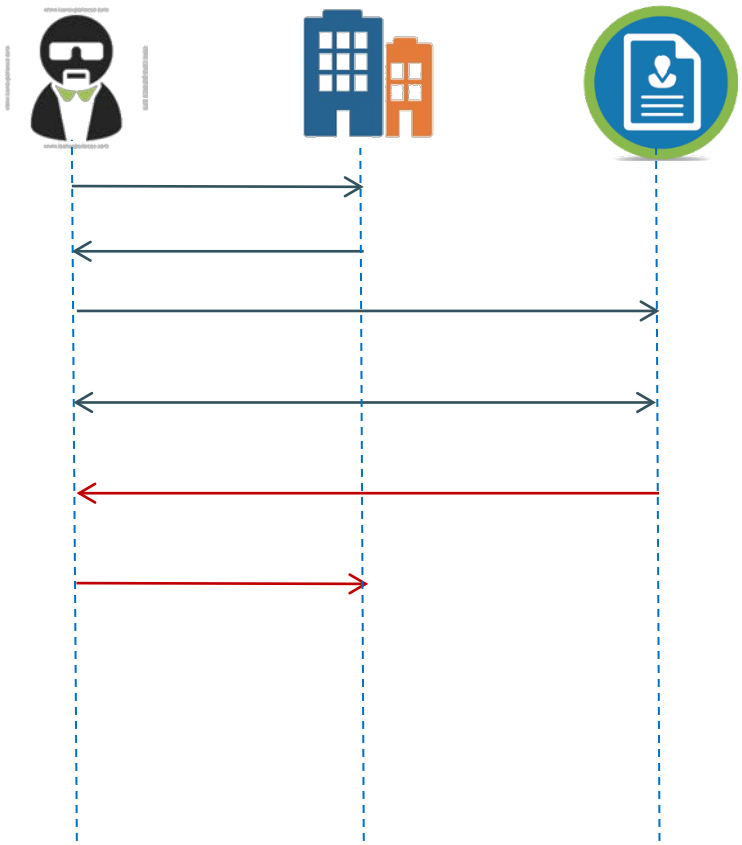
Типичан процес пријаве



- Корисник приступа заштићеном ресурсу
- Сервис преусмјерава корисника ка добављачу идентитета са захтјевом да се пријави (захтјев за аутентикацију)
- Корисник се пријави код добављача идентитета (аутентикација)
- Уколико постоји SSO сесија преузимају се подаци од претходне аутентикације

Протоколи за идентитете

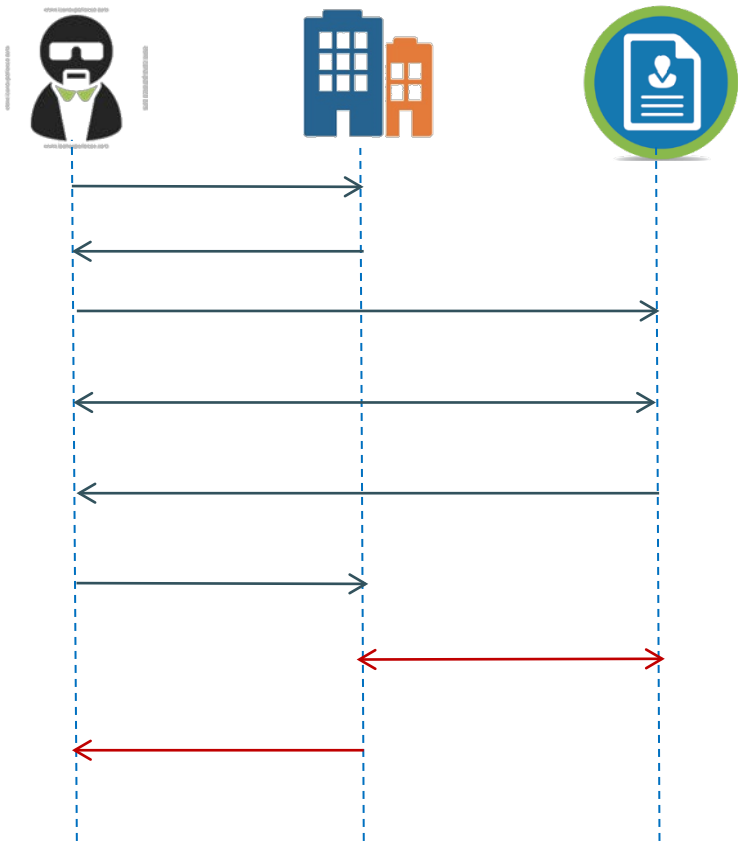
Типичан процес пријаве



- Корисник приступа заштићеном ресурсу
- Сервис преусмјерава корисника ка добављачу идентитета са захтјевом да се пријави (захтјев за аутентикацију)
- Корисник се пријави код добављача идентитета (аутентикација)
- Уколико постоји SSO сесија преузимају се подаци од претходне аутентикације
- Добављач идентитета преусмјерава корисника на изворни сервис (аутентикациони одговор)

Протоколи за идентитете

Типичан процес пријаве



- Корисник приступа заштићеном ресурсу
- Сервис преусмјерава корисника ка добављачу идентитета са захтјевом да се пријави (захтјев за аутентикацију)
- Корисник се пријави код добављача идентитета (аутентикација)
- Уколико постоји SSO сесија преузимају се подаци од претходне аутентикације
- Добављач идентитета преусмјерава корисника на изворни сервис (аутентикациони одговор)
- Сервис провјерава исправност и важење одговора (верификација)
- Сервис дозвољава приступ кориснику

Протоколи за идентитете

Типични протоколи

- SAML
- OAuth 2.0
- OpenID Connect
- XACML

Протоколи за идентитете

Примјер аутентикационих токена

OpenID Connect

```
POST /token HTTP/1.1
Host: moa-id.gv.at
Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW
Content-Type: application/x-www-form-urlencoded
grant_type=authorization_code
&code=SplxlOBeZQQYbYS6WxSbIA
&redirect_uri=https%3A%2F%2Fonline%2Eapplikation%2Egv%2Eat
```

```
HTTP/1.1 200 OK
Content-Type: application/json
{
"access_token":"SIAV32hkKG",
"token_type":"Bearer",
"id_token" : {
  "sub":"12345==",
  "given_name": "Max", "family_name": "Mustermann"
  "birthdate": "01-01-1990", "gender":"M"
}
```

SAML


```
[illegible]
```

Примјер аутентикационих токена

OpenID Connect

https://moa-id.gv.at/authorize
?response_type=code
&client_id=s1jdkweo513
&redirect_uri=https%3A%2F%onlineapp.gv.at%2Fcb
&scope=openid%20profile
&state=af0123iwe

HTTP 1.1 302 Found
Location: https://onlineapp.gv.at/cb
?code=SplxlOBeZQQYbYS6WxSbIA
&state=af0ifjsldkj

SAML


```
<saml2p:AuthnRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
AssertionConsumerServiceIndex="1" AttributeConsumingServiceIndex="0"
Destination="https://demo.egiz.gv.at/demoportal_moaid-2.0/pvp2/post"
ID="_e1ecdd2d80062991f8f0f489dfc49441" IssueInstant="2013-08-13T14:13:29.392Z" Version="2.0">
<saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">demologin-pvp2-sso/main/</saml2:Issuer>
<ds:Signaturexmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethodAlgorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethodAlgorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<ds:ReferenceURI="#_e1ecdd2d80062991f8f0f489dfc49441">
<ds:Transforms>
<ds:TransformAlgorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:TransformAlgorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transforms>
<ds:DigestMethodAlgorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>qGqkR6stEnKFS04DQ6yx44CDzzo=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>GhvpD+urP2BwEaejBW3Y3dmdIKdFDR9AikVn0TAyWBg3d/+gYxBQ0JHPn/XCoHP6QQHbNHjfqf8
o2wJQrvX9WD/BPJHK2wwecbzPK2cCIco5bGqhGq+LKwHPesHu10nrIfj4T8lAHX4lPiYR5OEDMXtV1SvHfWIzXEBGh/M
yJtk2qAFDT4OfglneNk8hYPjcwNb8MwMME+tlR97snFMzkXI5tHSKB8LzGIPq+K2A0c06AX2LJiT8xaDscJTqqeaub4zIm6
haZ1LZX0qMH2jFJVVjAfYbV2BhdSs6aseTLSp+k2rlPJqvpds8PBN26I8KYbk/bwQIZ0hSSo//f+q2cw==</ds:SignatureValu
e>
<ds:KeyInfo>
<ds:KeyValue>
<ds:RSAKeyValue>
<ds:Modulus>nEPzKMh3TovnfBnTyv+TMYFsGep8Uil7iNbfVyfLoBfqRdeGDOk4es2qWkgB6az+kM/9Js2H06m4
pjEY7/RIjd0lMWqgi8eqdjiIMmbFQykkYYQhlZbvi8KqoBcCKzj5N3GY4qh8A5qN4y85Q3sZj23T
iiIY1rphE+ZTOHCm6CKeRso9jj409YHP1xAXfPvtIYx2TA1uuagxOmL75OC/hr7gcUm0tmuKiSeq
+TO4VZw2Q7K7YESZ1WkiBoG2i4cHdcBFKnVrGNtyxl6UkjWxXRJSU9aNLs5QxsE6iFwCvFoIO+IU
cVWxfFHqOGbRtAcRUb4fk+KFHE2o1DLmfwZaUQ==</ds:Modulus>
<ds:Exponent>AQAB</ds:Exponent>
</ds:RSAKeyValue>
</ds:KeyValue>
</ds:KeyInfo>
</ds:Signature>
<saml2:Subject xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
<saml2:NameID>demologin-pvp2-sso/main/</saml2:NameID>
</saml2:Subject>
<saml2p:NameIDPolicy AllowCreate="true"
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"/>
<saml2p:RequestedAuthnContext>
<saml2:AuthnContextClassRef  comparison="minimum"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">http://www.stork.gov.eu/1.0/citizenQAALevel/4</saml2:AuthnCon
textClassRef>
</saml2p:RequestedAuthnContext>
</saml2p:AuthnRequest>
```

Питања?