A Kerberos-tól az OpenID Connect-ig

PPKE, ITK

Csapodi Márton

A Kerberos célja

forrás:
http://technet.microsoft.com/en-us/library/cc772815(v=ws.10).aspx
http://www.kerberos.org/software/tutorial.html
http://www.rfc-editor.org/rfc/rfc4120.txt

„Kerberos is an authentication protocol for trusted hosts on untrusted networks”

célok:

- felhasználó (kliens gép) hitelesítése az alkalmazás szerverek felé
- a felhasználói jelszó nem utazik, nem tárolódik (csak titkosítva a szerveren)
- központi felhasználó menedzsment
- single-sign-on
- kölcsönös azonosítás (opció)
- titkosított kommunikáció (opció)

Kerberos fogalmak / 1

realm/domain: Tartomány, melyben a kliensek egyetlen autentikációs szerverhez kapcsolódnak. Az igénybe vett szolgáltatás más tartományban is lehet (cross-domain autentikáció).

principal: Felhasználó vagy szolgáltatás a tartományon belül, egyedi névvel.

ticket: Jegy, melyet a kliens mutat be az igénybe vett szolgáltatásnak az autentikáció során. Tartalma titkosítva van a szolgáltatás szimmetrikus kulcsával (melyet a ticket kibocsátója ismer, de a kliens nem). Tartalma: kliens principal, szolgáltatás principal egyedi neve, kliens IP cím (opcionális), érvényesség kezdete, érvényesség időtartama, session kulcs. A ticket bemutatásakor igazolni kell a session kulcs ismeretét (authenticator).

session key: A ticket kibocsátója hozza létre, és külön titkosítja a kliens és a szolgáltatás szimmetrikus titkosító kulcsával. Ennek ismerete a (kölcsönös) autentikáció alapja a kliens és a szolgáltatás között.

authenticator: Hitelesítő adat, melyet a kliens a ticket bemutatásával párhuzamosan ad át a szolgáltatásnak. A kliens principal egyedi nevét és az időpontot tartalmazza a session kulccsal titkosítva.

Kerberos fogalmak / 2

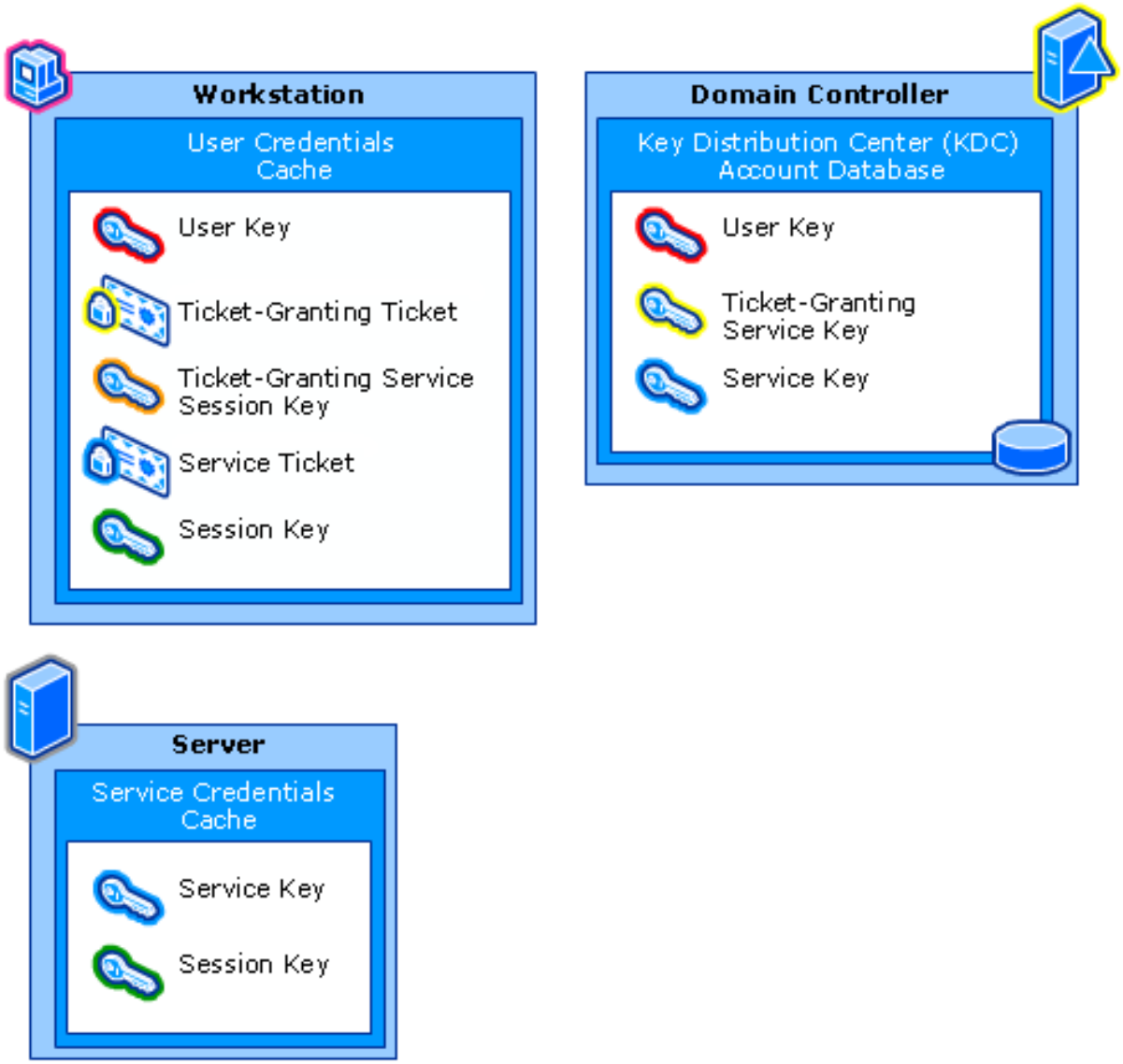
Key Distribution Center (KDC): Az adott tartomány autentikációs szolgáltatása, mely három részből áll: Database, Authentication Server és Ticket Granting Server.

Database: A tartomány prinicipal-jait, azok szimmetrikus kulcsát és a principal, valamint a ticket-ek érvényességi időit tartalmazza. (Titkosítva egy master kulccsal.)

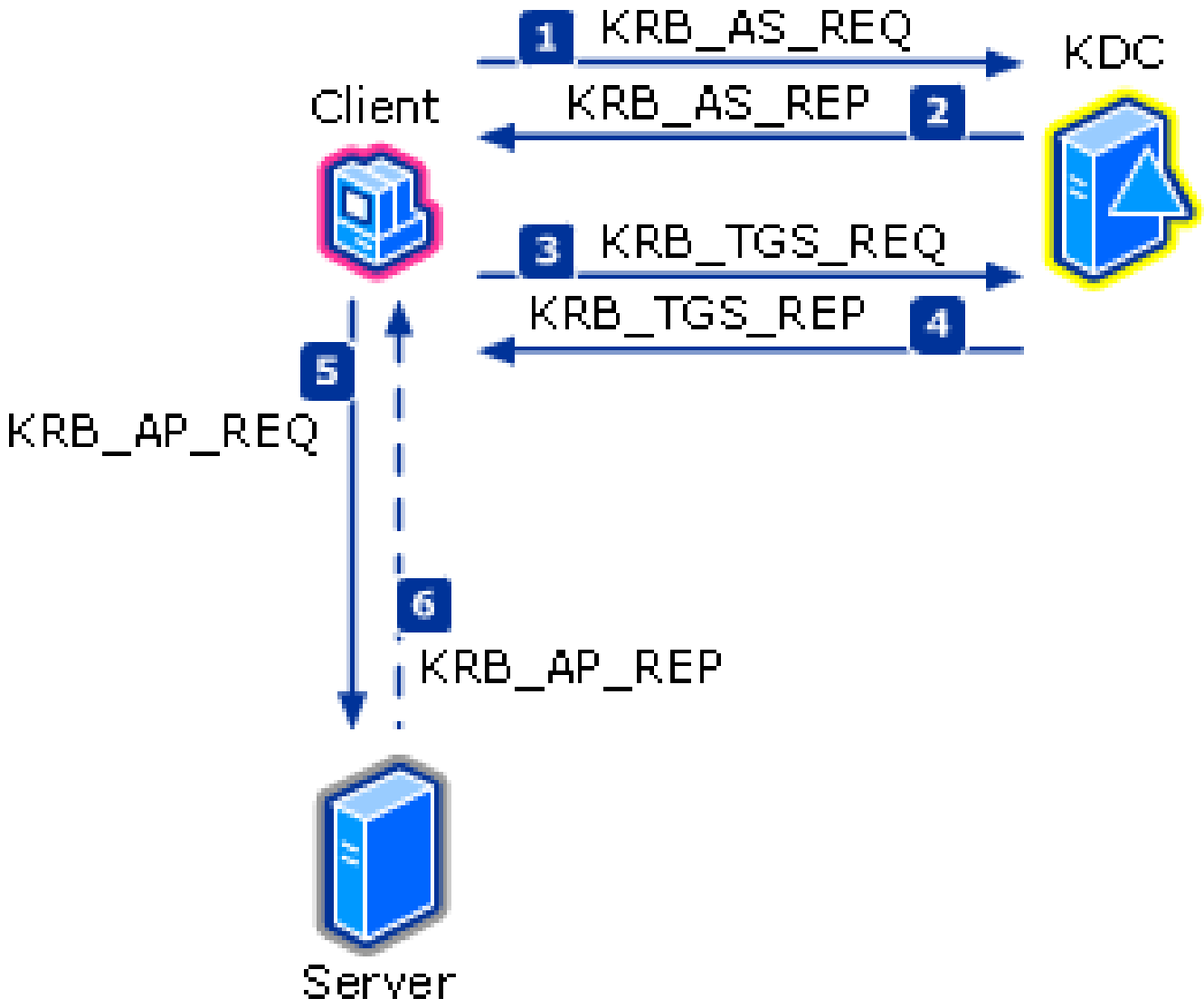
Authentication Server (AS): A még be nem jelentkezett felhasználó kezdeti autentikációját (jelszó ellenőrzését) végzi. A sikeres autentikáció eredménye egy Ticket Granting Ticket (TGT) átadása. A ticket-ek kiadása a TGT alapján történik, nem kell újra jelszót megadni.

Ticket Granting Server (TGS): A klienstől kapott érvényes TGT alapján átadja az adott szolgáltatáshoz kapcsolódó ticket-et.

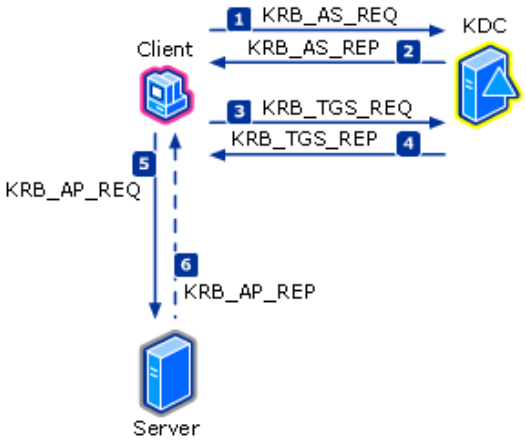
Kerberos adatok



Kerberos üzenetek

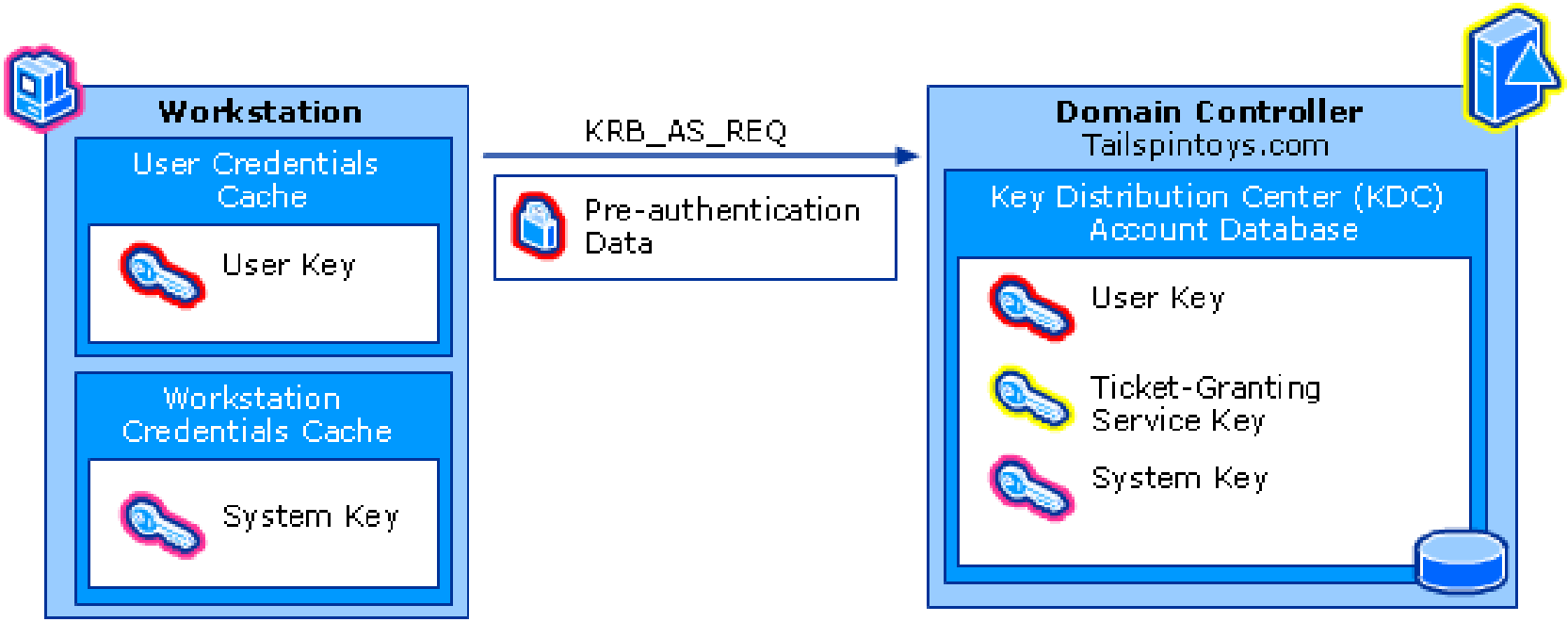


Kerberos autentikáció / 1

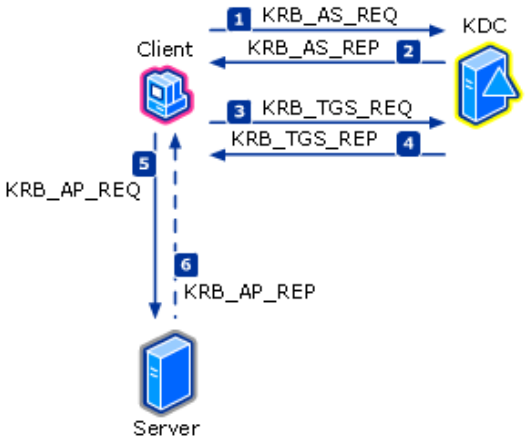


tartalma:

- kliens principal neve
- tartomány neve
- időpecsét titkosítva (User Key)

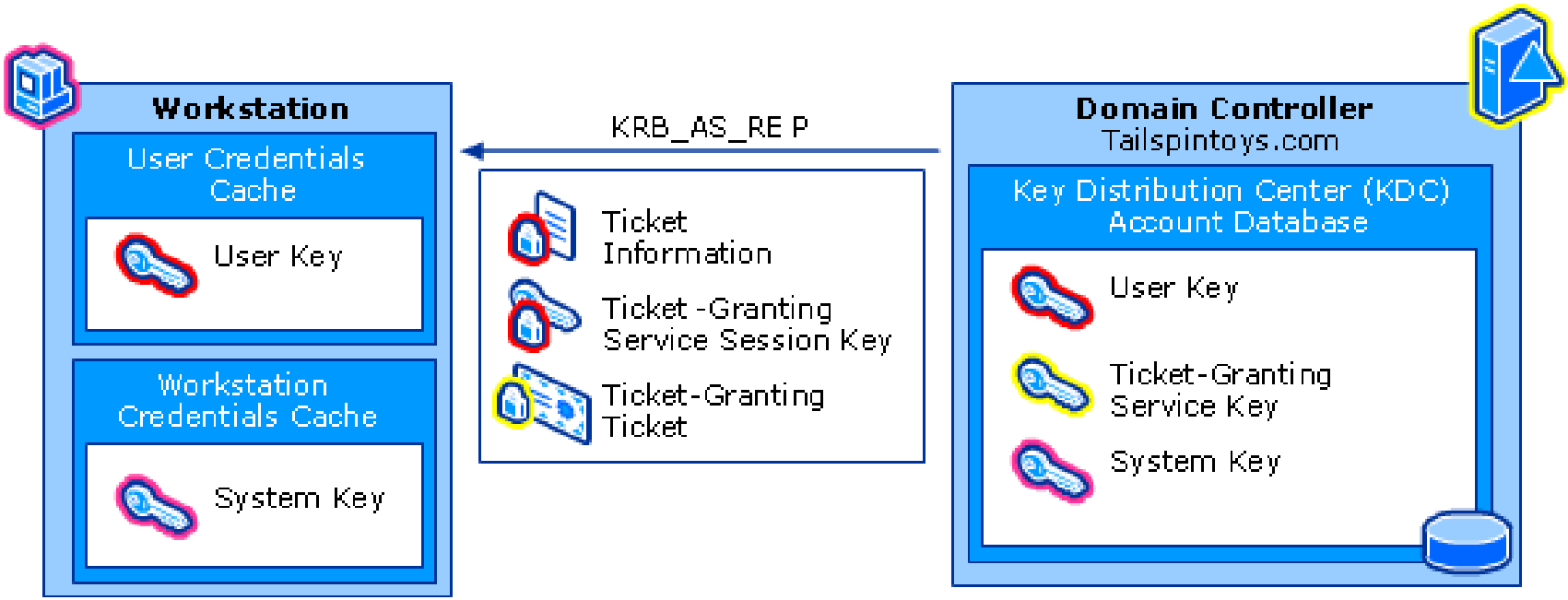


Kerberos autentikáció / 2

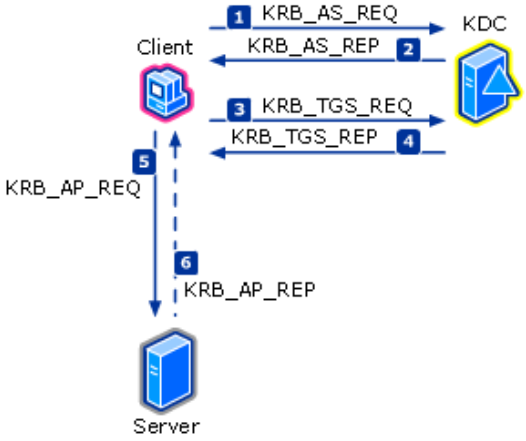


tartalma:

- TGT titkosítva (TGS Key)
- TGT részleges tartalma titkosítva (User Key) - érvényességi időadatok miatt
- TGS session kulcs titkosítva (User Key) - későbbi TGS kommunikációhoz

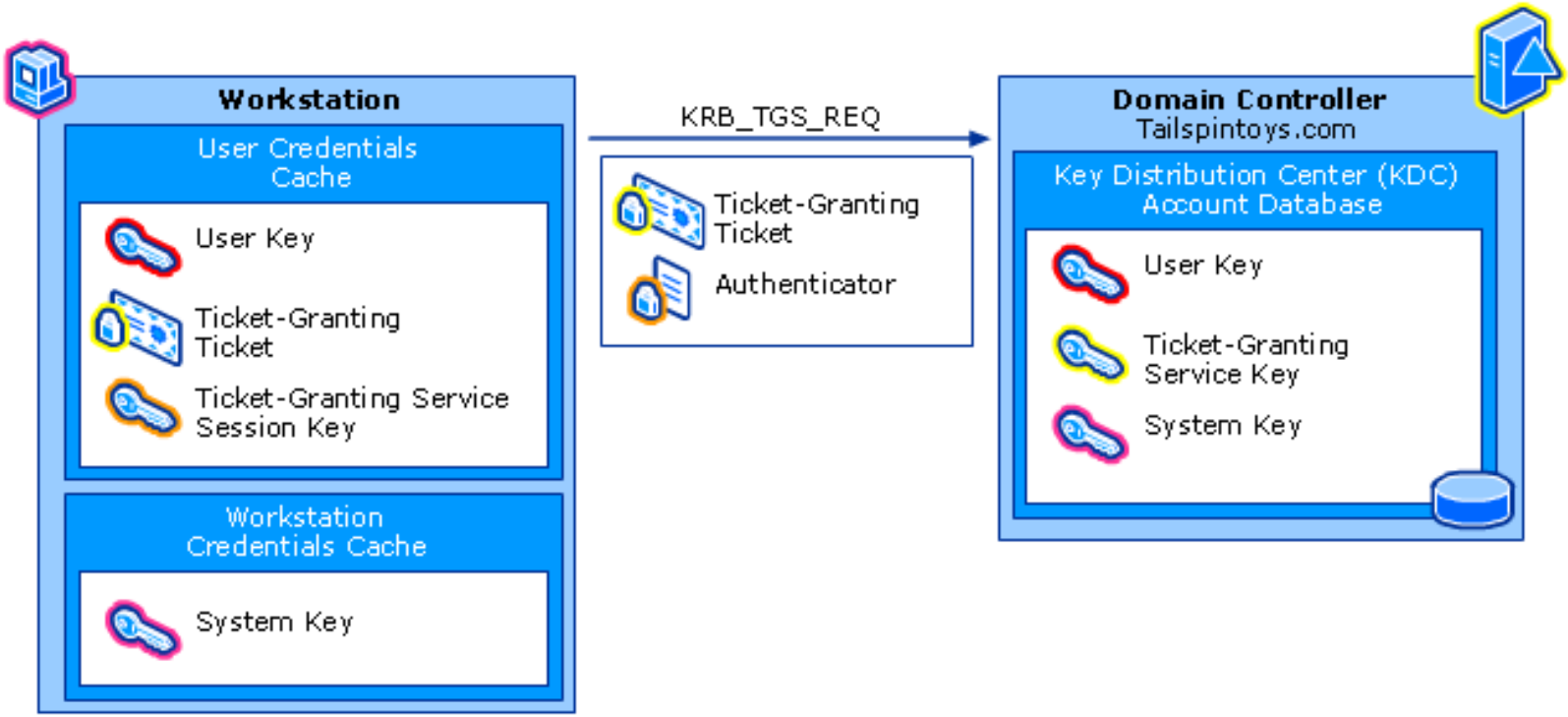


Kerberos workstation logon / 1

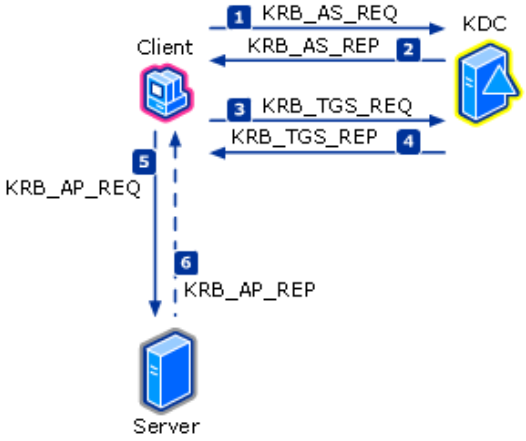


tartalma:

- workstation principal neve, tartomány neve
- TGT titkosítva (TGS Key) - ennek része a TGS session kulcs
- authenticator: user principal neve + időbélyegző titkosítva (TGS session key)

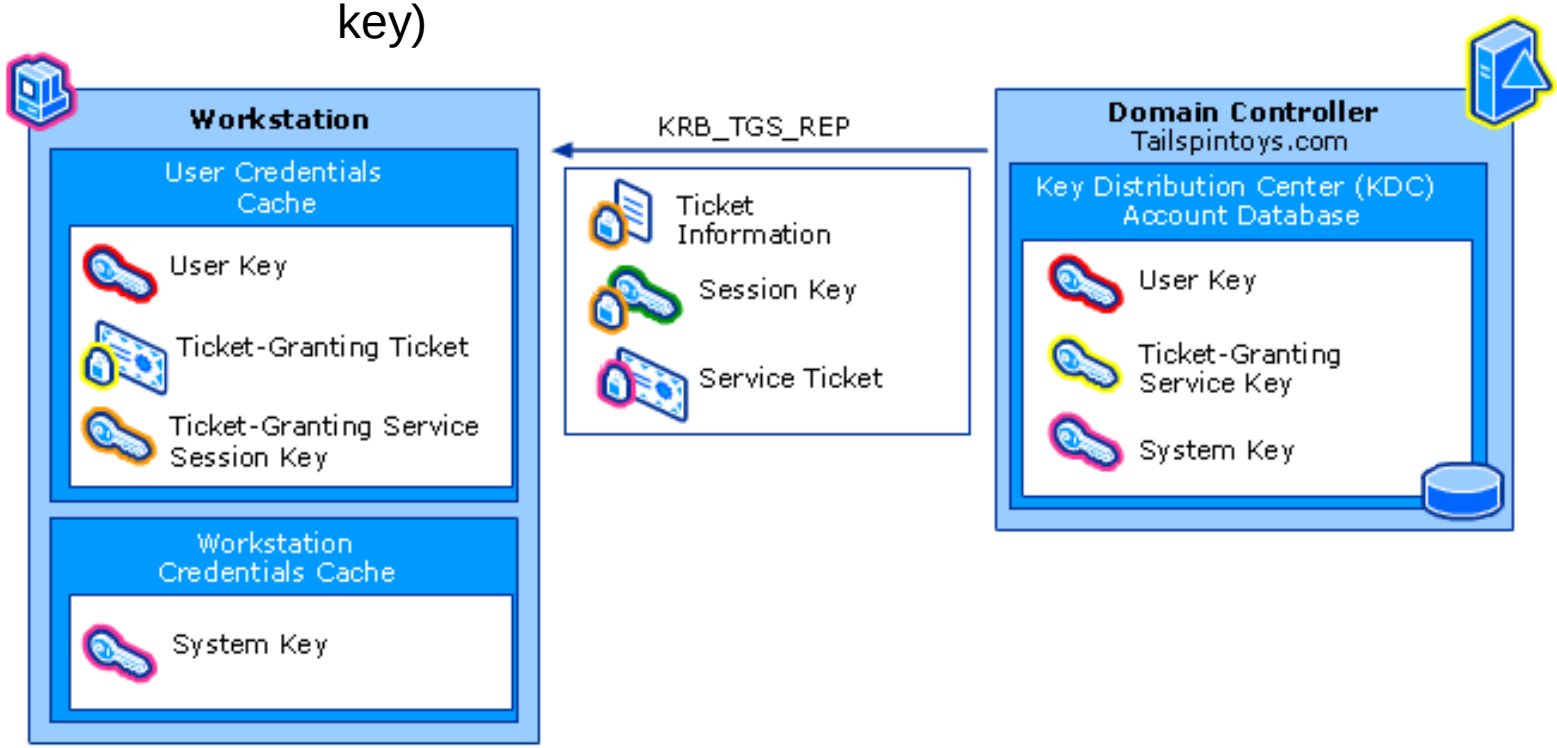


Kerberos workstation logon / 2

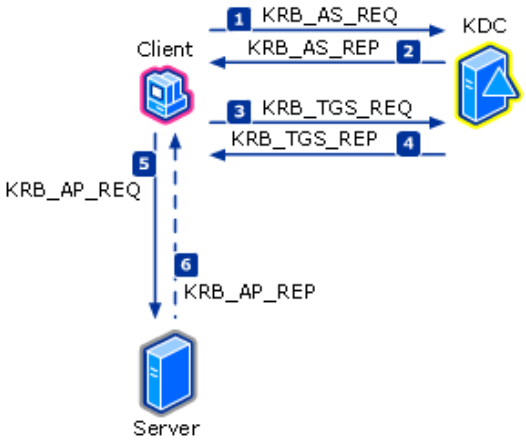


tartalma:

- Service ticket titkosítva (wokstation system key) - ennek része a user és a workstation közt megosztott session kulcs
- a Service ticket tartalma + a user és a workstation közt megosztott session kulcs titkosítva (TGS session key)



Kerberos workstation logon / 3



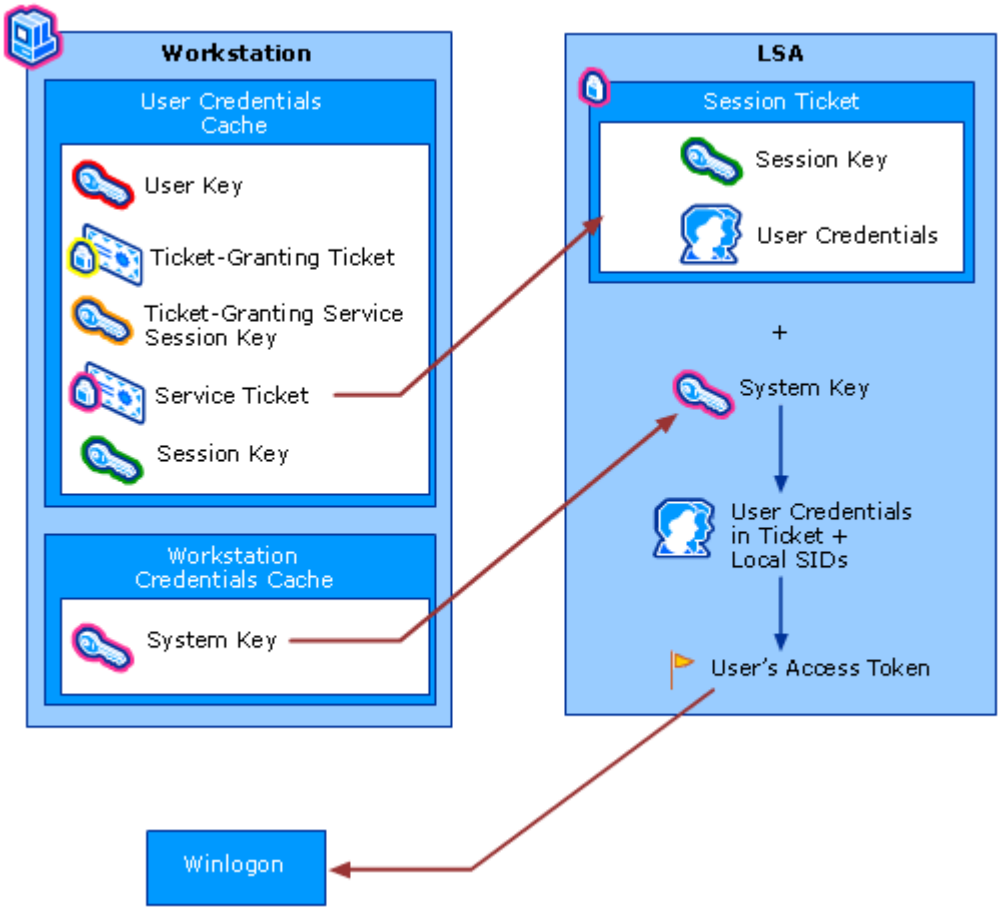
Local Security Authority feladata:

Service ticket dekódolása. Ez tartalmazza a User SID-jét: Security identifier (ez azonosítja a felhasználót, mert a név változhat).

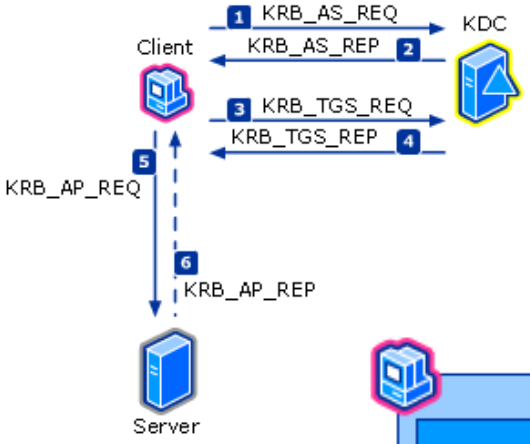
User jogosultságok (groups, privileges) lekérdezése

Access Token létrehozása, ami az adott felhasználó minden process-éhez hozzákapcsolódik

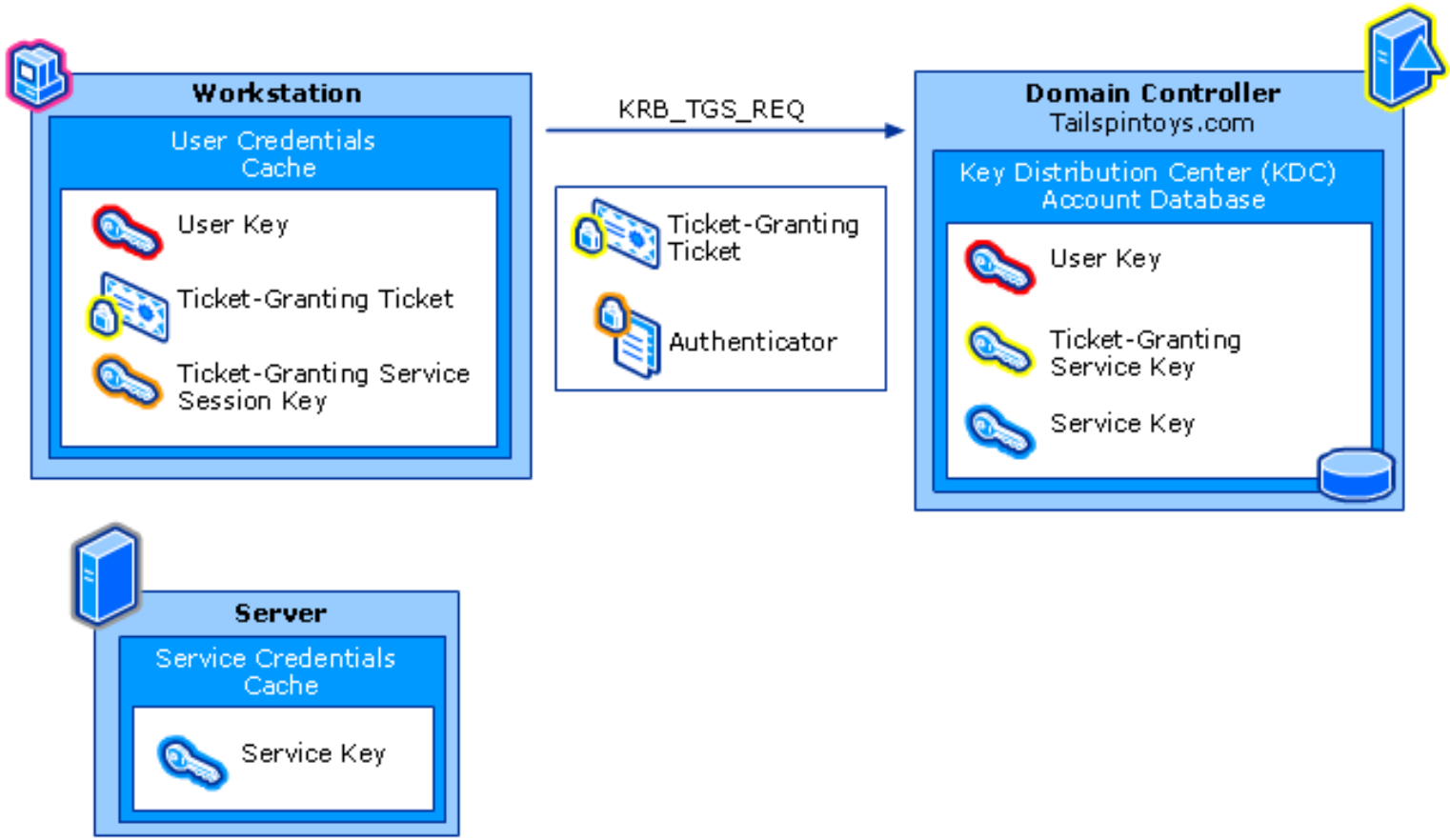
Windows shell indítása



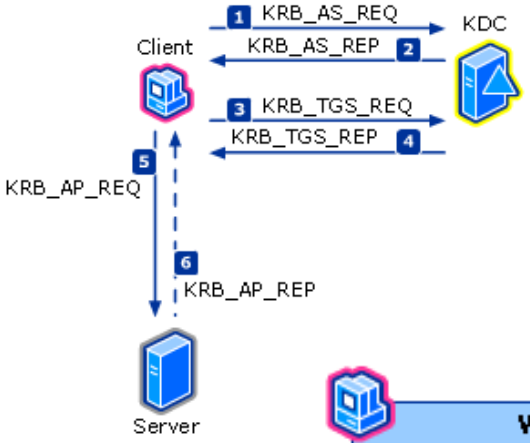
Kerberos szolgálatás logon / 1



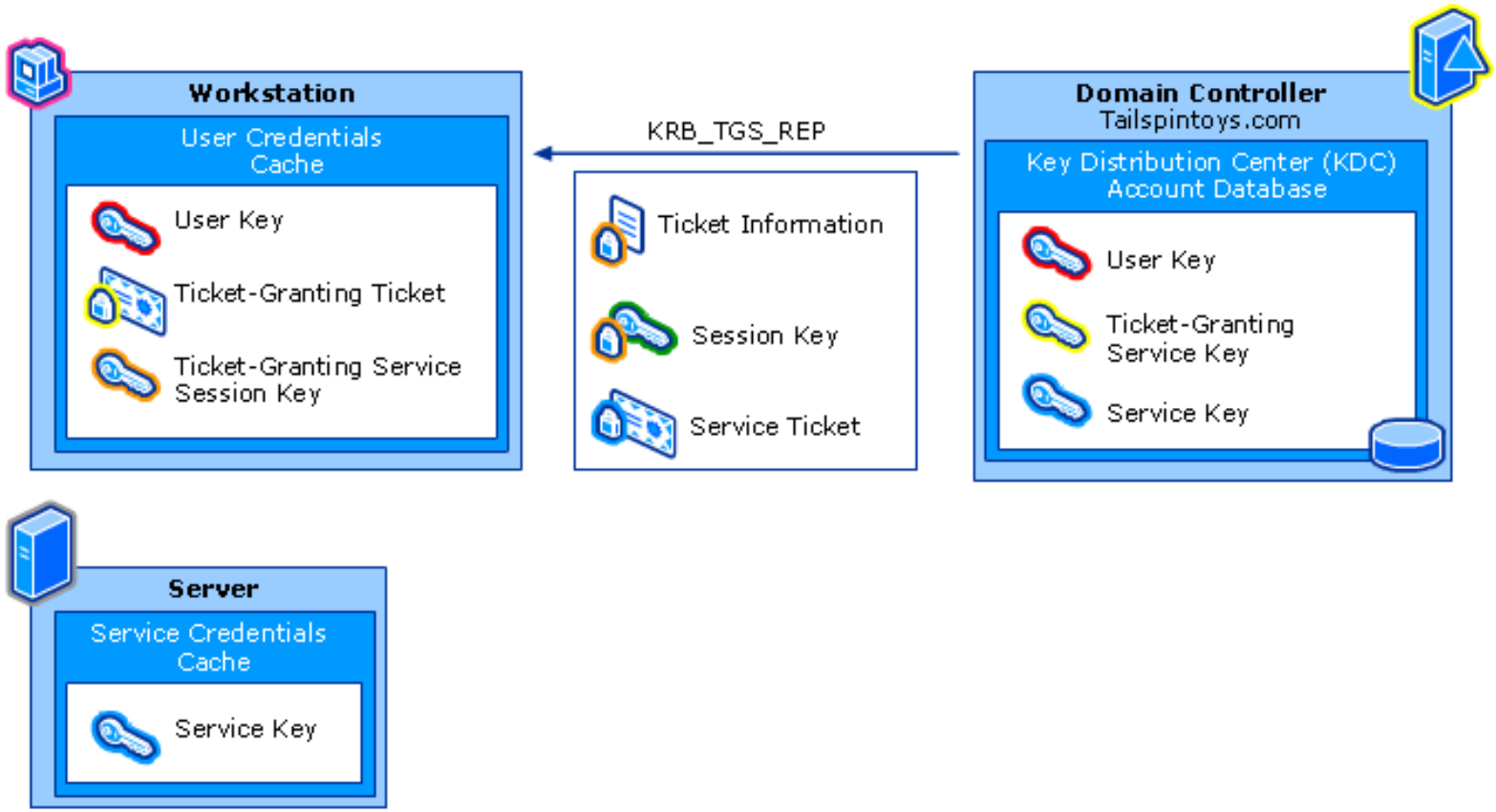
tartalma ugyanaz, mint a wokstation logon esetén, de a szolgáltatás principal neve és domain neve szerepel benne



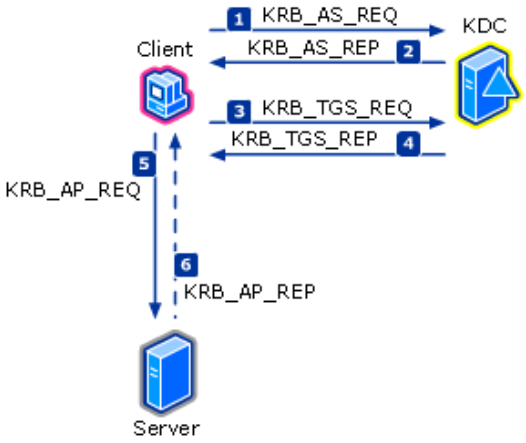
Kerberos szolgáltatás logon / 2



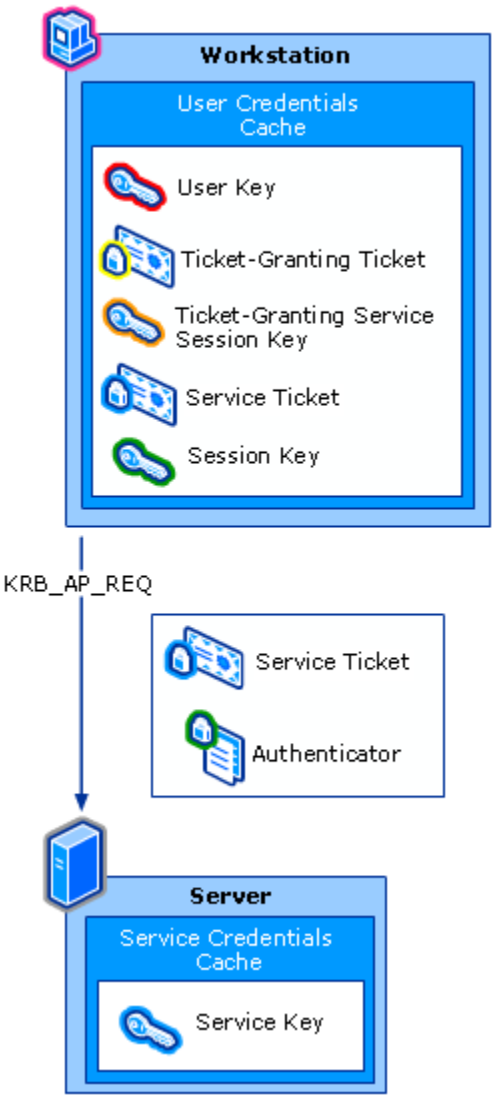
tartalma ugyanaz, mint a workstation logon esetén, de a ticket a szolgáltatás statikus kulcsával van titkosítva

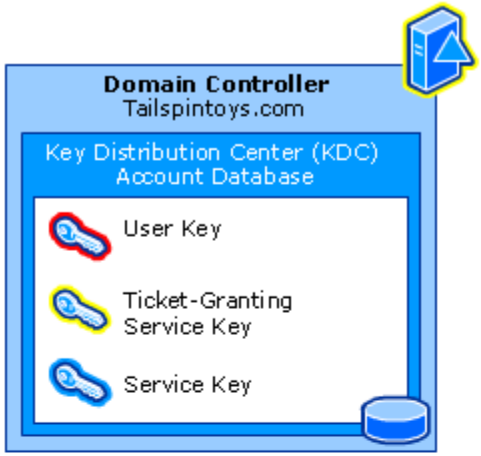


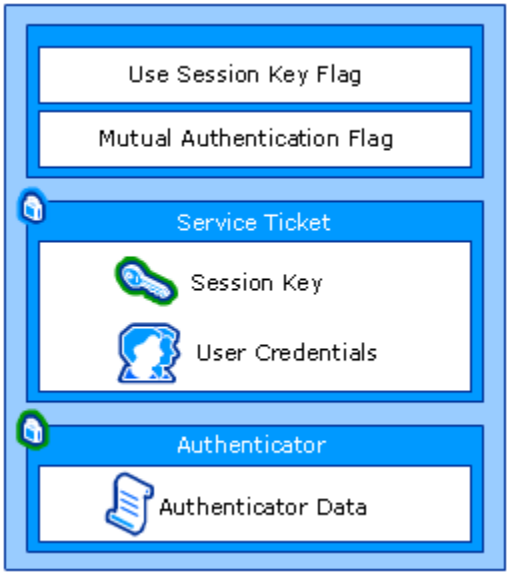
Kerberos szolgáltatás logon / 3



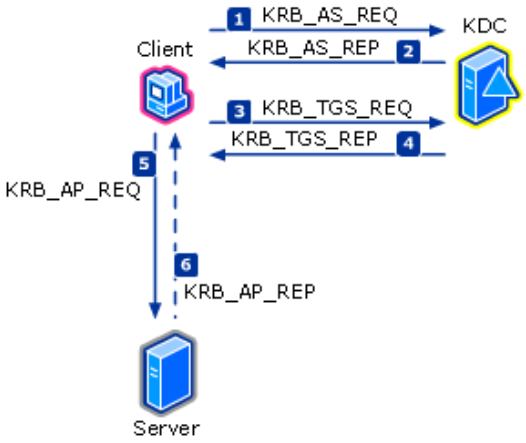
- Ticket information tartalmazza a flag-eket: titkosítás, szerver hitelesítés
- Service ticket tartalmazza a Service session kulcsot titkosítva (statikus Service key)
- authenticator: user principal neve + időbélyegző titkosítva (Service session key)







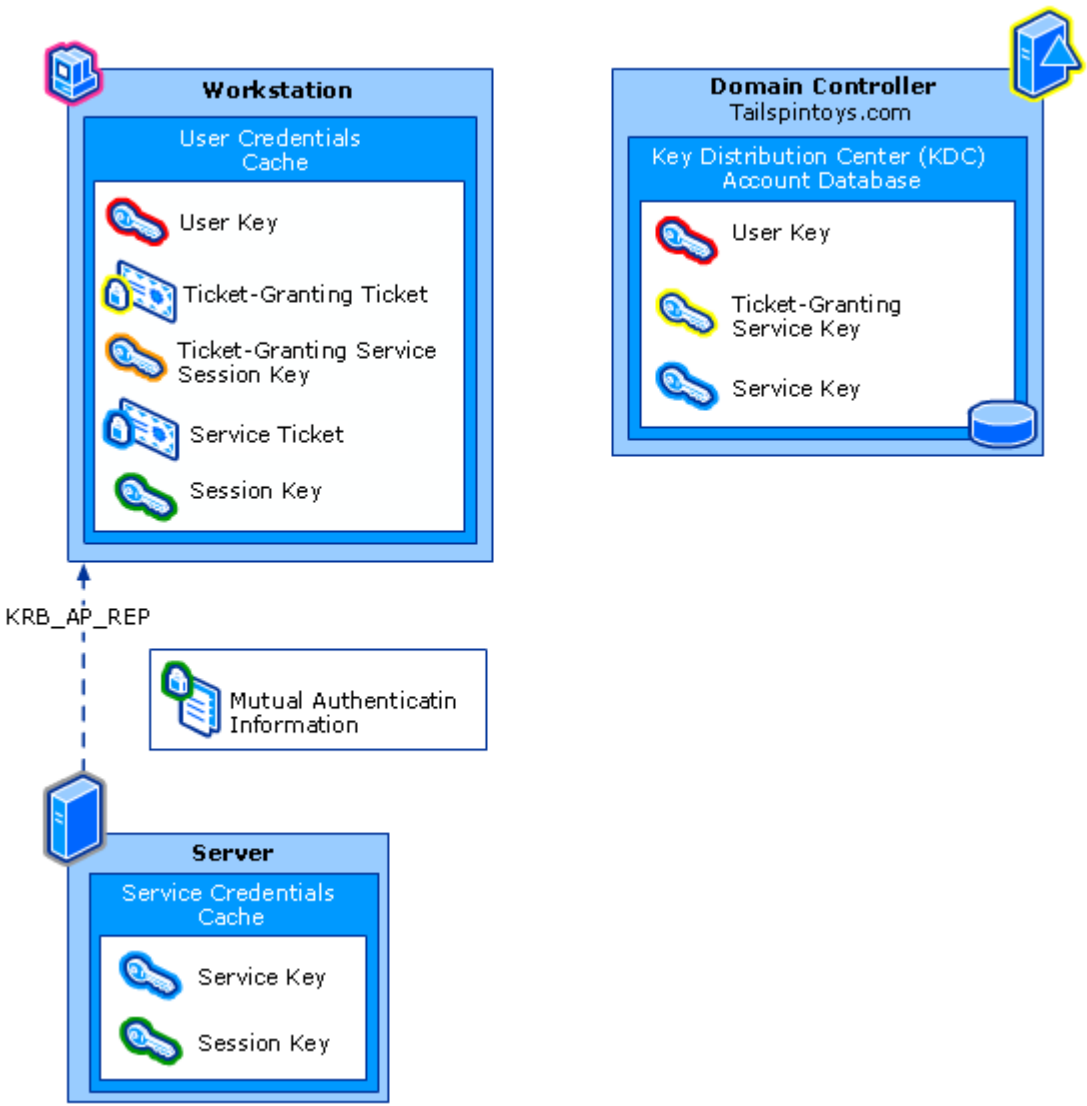
Kerberos szolgáltatás logon / 4



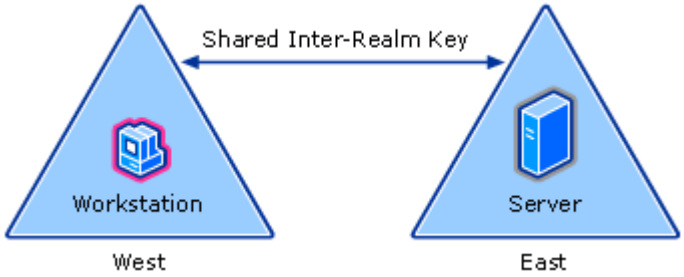
Opcionális lépés.

A KRB_AP_REQ-ben megadott időpecsétet titkosítja a Session kulccsal.

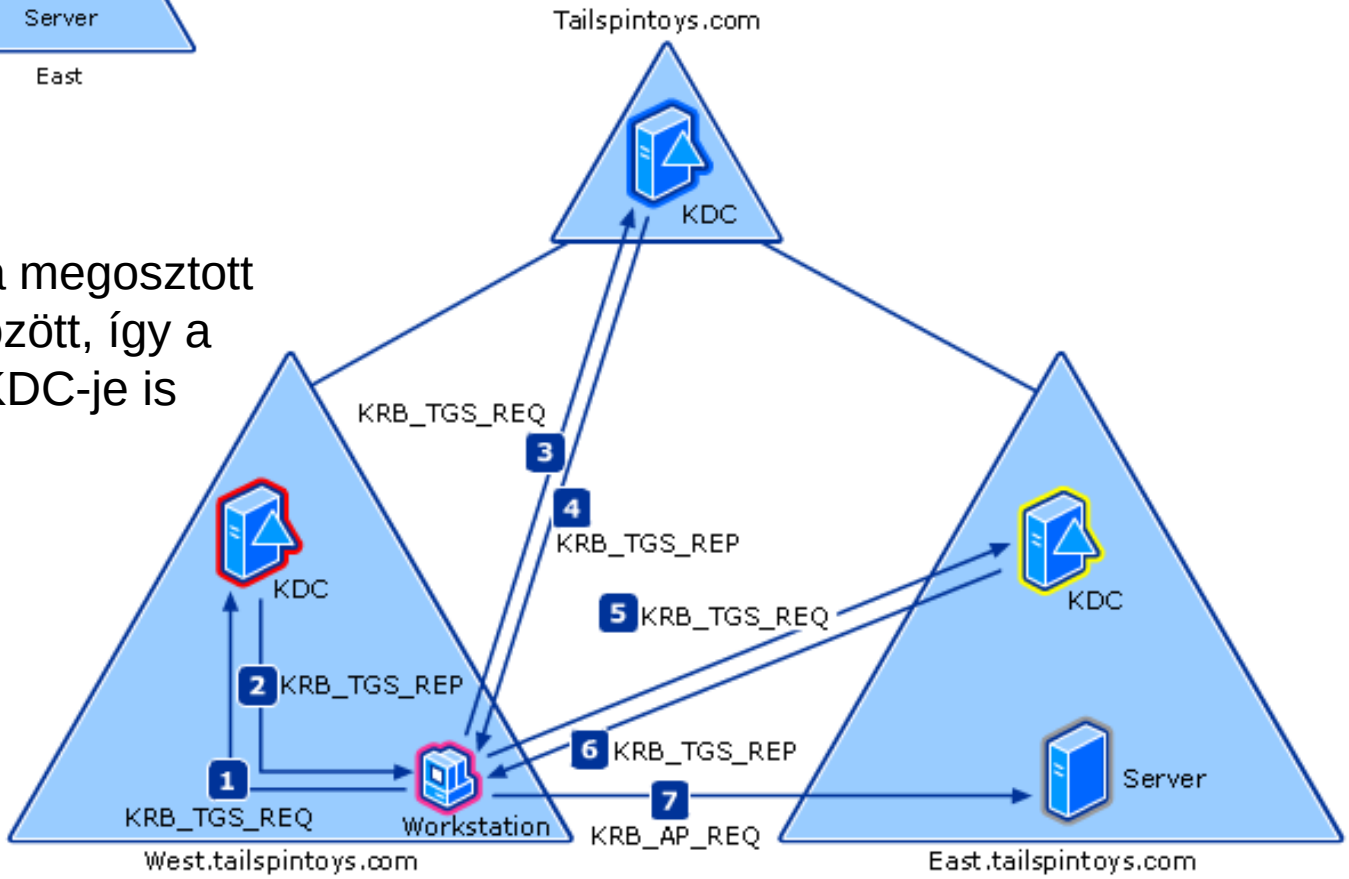
A kliens összeveti a két időpecsétet ellenérzéskor.



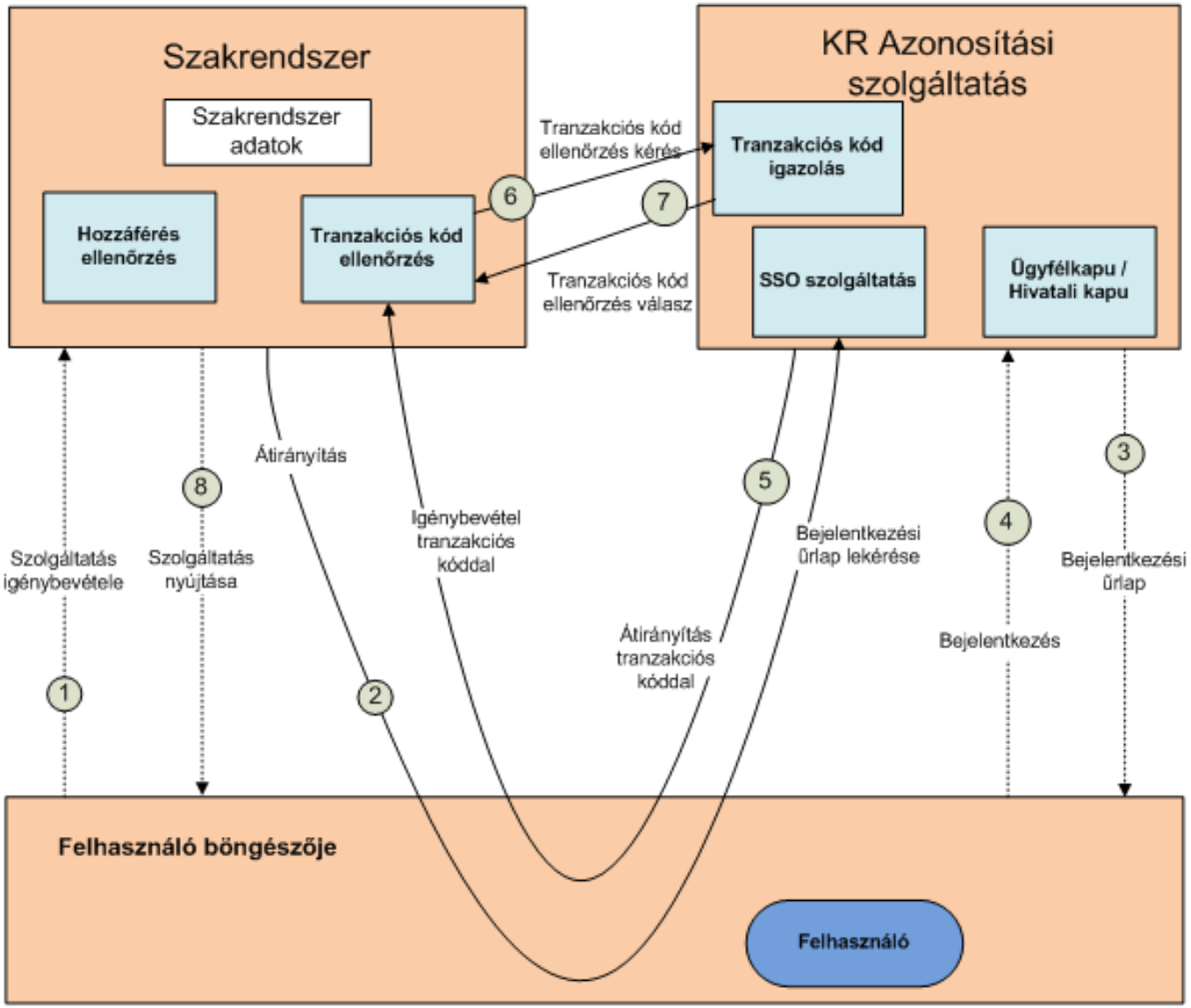
Tartományok közti autentikáció



A TGT titkosító kulcsa megosztott a két tartomány között, így a másik tartomány KDC-je is dekódolni tudja.



mo.hu (régi ügyfélkapu) SSO



HTTP alapok

HTTP alapok:

https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol

HTTP cookie alapok:

https://en.wikipedia.org/wiki/HTTP_cookie

HTTP redirect alapok:

https://en.wikipedia.org/wiki/HTTP_302

https://en.wikipedia.org/wiki/HTTP_303

https://en.wikipedia.org/wiki/Meta_refresh

HTTP redirect

HTTP redirect status codes 3xx:

- 301 moved permanently
- 302 found (HTTP 1.0: temporary redirect volt, de megváltozott az értelme)
- 303 see other (HTTP 1.1, csak GET-tel)
- 307 temporary redirect (HTTP 1.1, ugyanazzal a metódussal)

```
HTTP/1.1 301 Moved Permanently
Location: http://www.example.org/
Content-Type: text/html
Content-Length: 174

<html>
<head>
<title>Moved</title>
</head>
<body>
<h1>Moved</h1>
<p>This page has moved to <a href="http://www.example.org/">http://www.example.org/</a>.</p>
</body>
</html>
```

mo.hu login / 1

Kérés:

```
GET https://magyarorszag.hu/ HTTP/1.1
Host: magyarorszag.hu
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: hu-HU,hu;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Válasz:

```
HTTP/1.1 200 OK
Date: Thu, 23 Feb 2017 07:44:01 GMT
Set-Cookie: JSESSIONID=3D97B54A31BC4812BF8D40932DE85787.portal3; Path=/; Secure
Content-Type: text/html;charset=UTF-8
Keep-Alive: timeout=15, max=100
Connection: keep-alive
Transfer-Encoding: chunked
```

mo.hu login / 2

Kérés:

```
GET https://gate.gov.hu/sso/ap/ApServlet?partnerid=mohu HTTP/1.1
Host: gate.gov.hu
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: hu-HU,hu;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
Referer: https://magyarorszag.hu/
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

Válasz:

```
HTTP/1.1 200 OK
Date: Thu, 23 Feb 2017 07:44:34 GMT
Set-Cookie: JSESSIONID=D0719722E5F6614A412D89E87153AB33.sso2; Path=/
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Type: text/html;charset=UTF-8
Content-Length: 7293
Keep-Alive: timeout=15, max=100
Connection: keep-alive
```

mo.hu login / 3

Kérés:

```
POST https://gate.gov.hu/sso/ap/ApServlet HTTP/1.1
Host: gate.gov.hu
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: hu-HU,hu;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
Referer: https://gate.gov.hu/sso/ap/ApServlet?partnerid=mohu
Cookie: JSESSIONID=D0719722E5F6614A412D89E87153AB33.sso2
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 65

partnerid=mohu&target=&felhasznaloNev=          &jelszo=
```

Válasz:

```
HTTP/1.1 302 Moved Temporarily
Date: Thu, 23 Feb 2017 07:44:52 GMT
Content-Length: 0
Location: https://gate.gov.hu/sso/ap/ApServlet
Keep-Alive: timeout=15, max=100
Connection: keep-alive
Content-Type: text/plain; charset=UTF-8
```

mo.hu login / 4

Kérés:

```
GET https://gate.gov.hu/sso/ap/ApServlet HTTP/1.1
Host: gate.gov.hu
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: hu-HU,hu;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
Referer: https://gate.gov.hu/sso/ap/ApServlet?partnerid=mohu
Cookie: JSESSIONID=D0719722E5F6614A412D89E87153AB33.sso2
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

Válasz:

```
HTTP/1.1 200 OK
Date: Thu, 23 Feb 2017 07:44:52 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Type: text/html;charset=UTF-8
Content-Length: 5212
Keep-Alive: timeout=15, max=99
Connection: keep-alive
```

```
<meta http-equiv="refresh" content="3;URL=../InterSiteTransfer?TARGET=&amp;PARTNER=mohu"/>
```

mo.hu login / 5

Kérés:

```
GET https://gate.gov.hu/sso/InterSiteTransfer?TARGET=&PARTNER=mohu HTTP/1.1
Host: gate.gov.hu
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: hu-HU,hu;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
Cookie: JSESSIONID=D0719722E5F6614A412D89E87153AB33.sso2
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

Válasz:

```
HTTP/1.1 302 Moved Temporarily
Date: Thu, 23 Feb 2017 07:44:56 GMT
Content-Length: 0
Location: https://ugyfelkapu.magyarorszag.hu/mohu_portlet_frame/auth/SSOLogin?SAMLart=J5xaw%2FsCqMi
Keep-Alive: timeout=15, max=98
Connection: keep-alive
Content-Type: text/plain; charset=UTF-8
```

```
portlet_frame/auth/SSOLogin?SAMLart=J5xaw%2FsCqMibaiJEarMO5bNtpJ2l1XccZC72MQamocQn62F9n59fA&TARGET=
```

mo.hu login / 6

Kérés:

```
GET https://ugyfelkapu.magyarorszag.hu/mohu_portlet_frame/auth/SSOLogin?SAMLart=J5xaw%2FsCgM
Host: ugyfelkapu.magyarorszag.hu
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: hu-HU,hu;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
Cookie: cssSize=0
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

Válasz:

```
HTTP/1.1 302 Moved Temporarily
Date: Thu, 23 Feb 2017 07:45:38 GMT
Set-Cookie: sso_auth=KmyK353jV3Efm/bmSe44Uv/fEgvNgA88M4iLLpokBFg=; Domain=magyarorszag.hu; Path=/; Secure
Set-Cookie: JSESSIONID=87EA18C81643BF5334D98798D460D3E7.portal3; Path=/; Secure
Location: https://ugyfelkapu.magyarorszag.hu
Content-Length: 0
Keep-Alive: timeout=15, max=100
Connection: keep-alive
Content-Type: text/plain; charset=UTF-8
```

mo.hu login / 7

Kérés:

```
GET https://ugyfelkapu.magyarorszag.hu/ HTTP/1.1
Host: ugyfelkapu.magyarorszag.hu
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: hu-HU,hu;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
Cookie: cssSize=0; sso_auth=KmyK353jV3Efm/bmSe44Uv/fEgvNgA88M4iLLpokBFg=; JSESSIONID=87EA18C81643BF
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

Válasz:

```
HTTP/1.1 302 Moved Temporarily
Date: Thu, 23 Feb 2017 07:45:38 GMT
Set-Cookie: JSESSIONID=87EA18C81643BF5334D98798D460D3E7.portal3; Path=/; Secure
pragma: no-cache
Cache-control: no-cache,no-store,must-revalidate
Location: https://ugyfelkapu.magyarorszag.hu/szolgaltatasok/tarhely/beerkezett
Content-Length: 0
Keep-Alive: timeout=15, max=99
Connection: keep-alive
Content-Type: text/plain; charset=UTF-8
```

mo.hu login / 8

Tranzakciós kód ellenőrzése:

A szakrendszerhez történő visszairányítás egyik paramétere a sikeres bejelentkezéskor generált, a bejelentkezés idején érvényes egyedi azonosító: a tranzakciós kód (SAMLart).

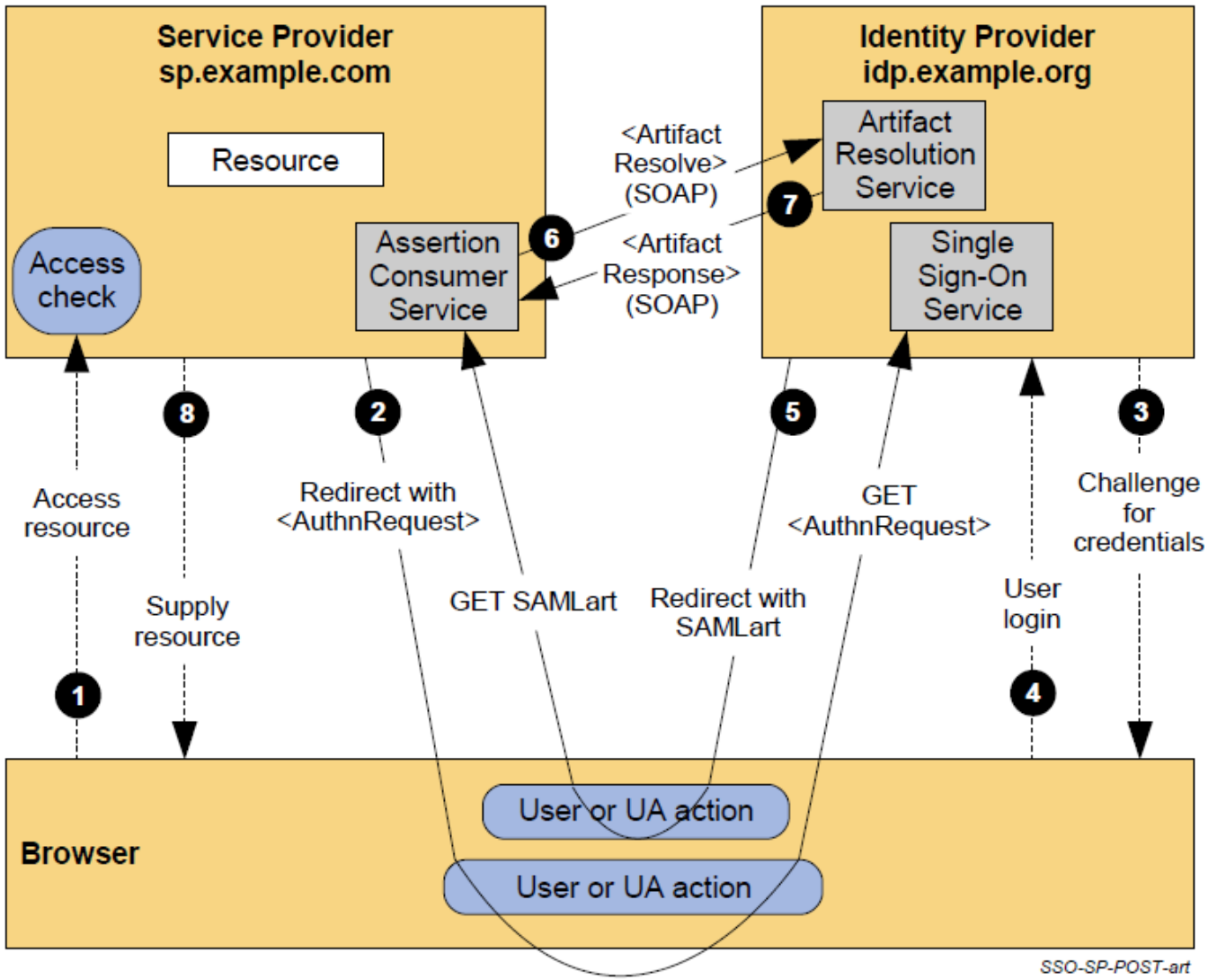
A szakrendszer ellenőrzi (szerver-szerver kommunikáció), hogy az adott felhasználó valóban sikeresen belépett a gate.gov.hu-n.

A tranzakciós kód ellenőrzési kérésre küldött válaszüzenetben a szakrendszer hozzájut az ügyfél ún. kapcsolati kódjához is, amely abban a rendszerben egyedi azonosítóként működik.

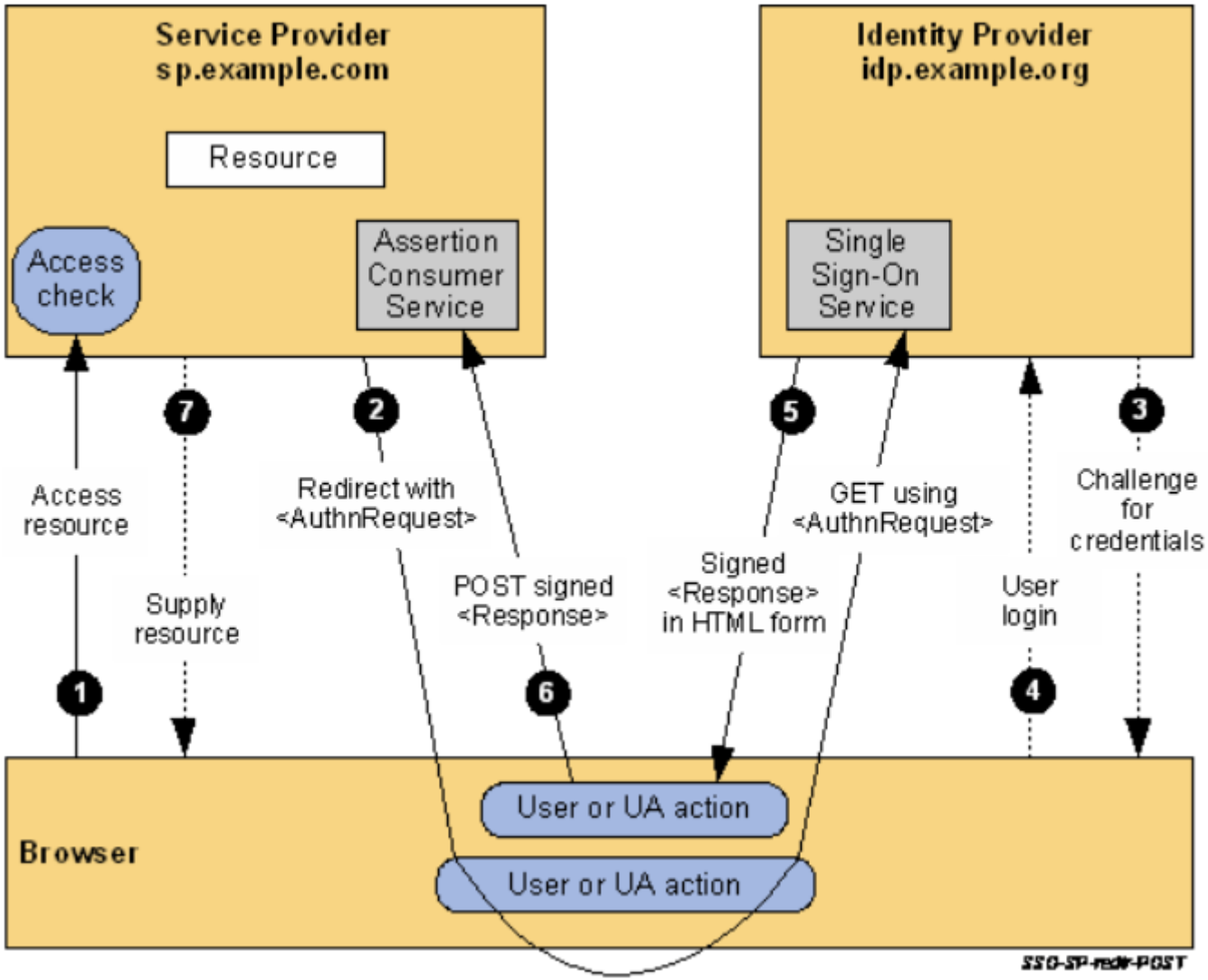
Viszontazonosítás:

A kapcsolati kód használatával a szakrendszer ellenőrizheti az adott felhasználó gate.gov.hu-n tárolt személyes adatait.

Security Assertion Markup Language (SAML) V2.0



SAML V2.0 a KAÜ esetében



kau.gov.hu login

Kérés:

```
POST https://kau.gov.hu/proxy/saml/authnrequest HTTP/1.1
Host: kau.gov.hu
Connection: keep-alive
Content-Length: 9928
Cache-Control: max-age=0
Origin: https://nyilvantarto.hu
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: https://nyilvantarto.hu/ugyseged/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,hu-HU;q=0.8,hu;q=0.6,en;q=0.4

SAMLRequest=PD94bWwgdmVyc2lvbjOiMS4wIiBlbmNvZGluZzOiVVRGLTgiPz4KPHNhbWwycDpBdXRoblJlcXVl%0D%0Ac3
```

kau.gov.hu login

SAMLRequest tartalma:


```
▼<saml2p:AuthnRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
 xmlns:xs="http://www.w3.org/2001/XMLSchema"
 AssertionConsumerServiceURL="https://www.nyilvantarto.hu/ugyseged/"
 Destination="https://kau.gov.hu/proxy/saml/authnrequest?lang=hu" ID="ID_e70459e4-
 88ec-45d6-810e-811b31556d55" IssueInstant="2017-03-09T15:48:19.772Z"
 ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Version="2.0">
   <saml2:Issuer
   xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">wu.kekkh.gov.hu</saml2:Issuer>
  ▶<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">...</ds:Signature>
  ▼<saml2p:Extensions>
    ▼<saml2:AttributeStatement xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
      ▶<saml2:Attribute Name="urn:eksz.gov.hu:1.0:ony:adatigenylo"
       NameFormat="urn:eksz.gov.hu:1.0:ony:adatigenylo">...</saml2:Attribute>
      ▶<saml2:Attribute Name="urn:eksz.gov.hu:1.0:ony:cel"
       NameFormat="urn:eksz.gov.hu:1.0:ony:cel">...</saml2:Attribute>
      ▶<saml2:Attribute Name="urn:eksz.gov.hu:1.0:ony:felhasznalo"
       NameFormat="urn:eksz.gov.hu:1.0:ony:felhasznalo">...</saml2:Attribute>
      ▶<saml2:Attribute Name="urn:eksz.gov.hu:1.0:ony:jogalap"
```

kau.gov.hu login

SAMLRequest tartalma:

```
▼<saml2:Attribute Name="urn:eksz.gov.hu:1.0:ony:szervezetkod"
 NameFormat="urn:eksz.gov.hu:1.0:ony:szervezetkod">
   <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:type="xs:string">KEKKH_WU</saml2:AttributeValue>
 </saml2:Attribute>
▼<saml2:Attribute Name="urn:eksz.gov.hu:1.0:4t"
 NameFormat="urn:eksz.gov.hu:1.0:4t">
   <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:nil="true" xsi:type="xs:string"/>
 </saml2:Attribute>
▶<saml2:Attribute Name="urn:eksz.gov.hu:1.0:felhasznalo_azonosito"
 NameFormat="urn:eksz.gov.hu:1.0:felhasznalo_azonosito">...</saml2:Attribute>
</saml2:AttributeStatement>
</saml2p:Extensions>
<saml2p:NameIDPolicy AllowCreate="false" Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent" SPNameQualifier="urn:eksz.gov.hu:1.0:rnytkk"/>
▼<saml2:Conditions xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
 ▼<saml2:AudienceRestriction>
   <saml2:Audience>urn:eksz.gov.hu:1.0:azonositas:kau:1</saml2:Audience>
 </saml2:AudienceRestriction>
```

kau.gov.hu login

AuthnRequest értelme:

A szakrendszer által, a felhasználó számára létrehozott és a KAÜ felé továbbítandó SAML v2.0 szabvány szerinti AuthnRequest üzenet tartalmazza az adott szakrendszerhez való hozzáférés feltételeit:

- végre kell hajtani a megfelelő felhasználó-hitelesítést és
- a kért típusú azonosítóadat lekérdezését.

A sikeres kommunikációhoz szükség van:

- a kérést küldő szakrendszer címére (akinek a válasz visszaküldésre kerül),
- egy egyedi tranzakció azonosítóra,
- az azonosítási szolgáltatás meghatározására.

kau.gov.hu login

AuthnRequest alá van írva (XML aláírás szabványnak megfelelően):

```
▼<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  ▼<ds:SignedInfo>
     <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
     <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    ▼<ds:Reference URI="#ID_e70459e4-88ec-45d6-810e-811b31556d55">
      ▼<ds:Transforms>
         <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
         signature"/>
        ▼<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
           <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
           PrefixList="xs"/>
         </ds:Transform>
       </ds:Transforms>
       <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
       <ds:DigestValue>QsDRNNAVqdssgp5gJfbf0sf3Bjk=</ds:DigestValue>
     </ds:Reference>
   </ds:SignedInfo>
  ▼<ds:SignatureValue>
     1vRmUCdYvLrsgcbh01z5BzJdltheIgDXDAKYpjki2Thz8IB4JXt6MG0sVpIW4uBpCydjAcyh9JsAe6wD
   </ds:SignatureValue>
```

kau.gov.hu login

AuthnRequest alá van írva (XML Signature szabványnak megfelelően):


```
<ds:KeyInfo>
  <ds:X509Data>
    <ds:X509Certificate>
      MIIHXjCCBkagAwIBAgIIbMyQynJvmtkwDQYJKoZIhvcNAQELBQAwgZYxCzAJBgNVBAYTAkhVMRE
      DwYDVQQHDAhCdWRhcGVzdDE8MDoGA1UECgwzTklTWiBOZW16ZXRpIEluZm9rb21tdW5pa8OhY2n
      s3MgU3pvbGfDoWx0YXTDsyBacnQuMTYwNAYDVQQDDC1NaW7FkXPDrXRldHQgVGFuw7pzw610dsO
      bnlraWFkw7MgdjIgLSBHT1YgQ0EwHhcNMTYwOTI4MDczNzA1WhcNMTcwOTI4MDczNzA1WjCBszE
      MAkGA1UEBhMCSFUxETAPBgNVBAcMCEJ1ZGFwZXN0MQ8wDQYDVQQKDAZLRUsgS0gxGTAXBgNVBAU
      EERPMjAxMzEyMDItMURPNzcxNTAzBgNVBAMMLFdlYmVzIMOcZ3lzZWfDqWQgU1AgQWzDocOtcsO
      IHRhbsO6c8OtdHbDoW55MQ0wCwYDVQQRDAQxMDk0MR8wHQYDVQQJDBZCYWzDoXpzIELDqWxhIHV
      Y2EgMzUuMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA6GMWHgEVNom/+S9kmkTreGR
      EUjbMQ0jwpyGtrjPQZ5rMHEDVu3VgoJX4bl2yCq/Qz0w02Z52XhnE1ZA5ahnnLTU9PlZyNrZb8/
      zd/Wo5w6kM7jf9yAR+h+yrxNqmMNkeHPVck4PYQ8qJ1c1Q6dgH2zrA9Iss4HmcBICcfvUEHijdj
      Lhd1flMJabDVPfYCkYbxXmPadUNXyM6Bf93oJqGWbRNMLWhPWqNsyz0mlsfdAeHcsMrgSGoQ5bd
      HhKAS9K13V5BU2DGZB4DfkQmTyNFnxbfdJeI2tmUTDBYFY135a3DylIFANJ/+iGYlaIzoiQfHqg
      h8S+yvhAutjc7wIDAQABo4IDjzCCA4swdQYIKwYBBQUHAQEEaTBnMDcGCCsGAQUFBzAChitodHR
      Oi8vcWNhLmhpdGVsZXMuZ292Lmh1L2Nlci9HT1ZDQS1RdjIuY2VyMCwGCCsGAQUFBzABhiBodHR
      Oi8vcW9jc3AuaGl0ZWxlcy5nb3YuaHUvb2NzcDAdBgNVHQ4EFgQUcSyCc3UWetOGLDnM9ZE8nMT
      fDQwDAYDVR0TAQH/BAIwADAfBgNVHSMEGDAWgBT0ozuPKXoxKM9ryIb4JqjL3SeIgDBIBggrBgE
```

kau.gov.hu login

Sikeres belépést követő visszairányítás:

```
POST https://www.nyilvantarto.hu/ugyseged/ HTTP/1.1
Host: www.nyilvantarto.hu
Connection: keep-alive
Content-Length: 32102
Cache-Control: max-age=0
Origin: https://kau.gov.hu
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/5
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: https://kau.gov.hu/proxy/saml/response
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,hu-HU;q=0.8,hu;q=0.6,en;q=0.4
Cookie: _ga=GA1.2.1976521315.1489074501; _gat=1

SAMLResponse=PD94bWwgdmVyc2lvbjOiMS4wIiBlbmNvZGluZzOiVVRGLTgiPz48c2FtbDJwOlJlc3BvbnNlIHht%0D%0A
OAbmNlIFVSSTOiI18yNDBlNTQOYzE3MDBjZmQzNWJjYWUyOWJhODVlYzhhYSIvPgogICAgICAgICAg%0D%0AICAgICA8L3h
```

kau.gov.hu login

SAMLResponse tartalma (aláírva, titkosítva):

```
▼<saml2p:Response xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol" Destination="kau.gov.hu"
 ID="ID_8ccf1ab6-3d90-4cf7-af62-8b8057148a22" InResponseTo="ID_51a722c5-5f13-4a05-ae9b-f63f61e8a1df"
 IssueInstant="2017-03-09T15:48:39.552Z" Version="2.0">
   <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">idp.gov.hu</saml2:Issuer>
 ▶<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">...</ds:Signature>
 ▼<saml2p:Status>
     <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
   </saml2p:Status>
 ▶<saml2:EncryptedAssertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">...
   </saml2:EncryptedAssertion>
 </saml2p:Response>
```

kau.gov.hu login

Titkosított adat és titkosított szimmetrikus kulcs (XML Encryption szabvány):

```
▼<saml2p:Response xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol" Destination="kau.gov.hu"
 ID="ID_8ccf1ab6-3d90-4cf7-af62-8b8057148a22" InResponseTo="ID_51a722c5-5f13-4a05-ae9b-f63f61e8a1df"
 IssueInstant="2017-03-09T15:48:39.552Z" Version="2.0">
   <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">idp.gov.hu</saml2:Issuer>
 ▶<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">...</ds:Signature>
 ▶<saml2p:Status>...</saml2p:Status>
 ▼<saml2:EncryptedAssertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
   ▶<xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    Id="_ea58bcbe55e27d99c65cea3b60314105" Type="http://www.w3.org/2001/04/xmlenc#Element">...
    </xenc:EncryptedData>
   ▶<xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    Id="_76d8e1fcf52e45e7cecaa80801ec325b" Recipient="ID_2481511d-bf02-43c0-bd67-56abc1d8103f">...
    </xenc:EncryptedKey>
  </saml2:EncryptedAssertion>
 </saml2p:Response>
```

kau.gov.hu login

Titkosított adat:


```
<xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
Id="_ea58bcbe55e27d99c65cea3b60314105" Type="http://www.w3.org/2001/04/xmlenc#Element">
  <xenc:EncryptionMethod xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
  Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="ID_7298dcf3-0f6c-4c7d-b8a1-
  c5c57562a2dc">
    <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"
    URI="#_76d8e1fcf52e45e7cecaa80801ec325b"/>
  </ds:KeyInfo>
  <xenc:CipherData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
    <xenc:CipherValue>
      v9/Y89veXDzB0uzAUra+2ejuPrZYSb4rNjDEM+nf12VKWigU+FbVgI5rI4e/d5wA/jZpcJAGSQzOQTOOxpEnZCzX
    </xenc:CipherValue>
  </xenc:CipherData>
</xenc:EncryptedData>
```

kau.gov.hu login

Titkosított szimmetrikus kulcs:


```
▼<xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
 Id="_76d8e1fcf52e45e7cecaa80801ec325b" Recipient="ID_2481511d-bf02-43c0-bd67-56abc1d8103f">
   <xenc:EncryptionMethod xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
   Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
  ▼<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="ID_2481511d-bf02-43c0-bd67-
   56abc1d8103f">
    ▼<ds:X509Data>
      ▼<ds:X509Certificate>
          MIIHOjCCBiKgAwIBAgIIXoA3sQ3Z4WIwDQYJKoZIhvcNAQELBQAwgbQxCzAJBgNVBAYTAkhVMREw
          DwYDVQQHDAhCdWRhcGVzdDE8MDoGA1UECgwzTklTWiBOZW16ZXRpIEluZm9rb21tdW5pa8OhY2nD
          s3MgU3pvbGfDoWx0YXTDsyBacnQuMVQwUgYDVQQDDEtUaXRrb3PDrXTDsyBUYW7DunPDrXR2w6Fu
          eWtpYWTDsyAtIEtvcm3DoW55emF0aSBIaXRlbGVzw610w6lzIFN6b2xnw6FsdGF0w7MwHhcNMTUw
          NjMwMTMwMzMwWhcNMTcwNjI5MTMwMzMwWjCBuTELMAkGA1UEBhMCSFUxETAPBgNVBAcMCEJ1ZGFw
          ZXN0MTwwOgYDVQQKDDNOSVNaIE5lbXpldGkgSW5mb2tvbW11bmlrw6FjacOzcyBTem9sZ8OhbHRh
          dMOzIFpydC4xGjAYBgNVBAUTEURPMjAxMzA5MTctMURPMTMwMRMwEQYDVQQDDAprYXUuZ292Lmh1
          MQ0wCwYDVQQRDAQxMDgxMRkwFwYDVQQJDBBDc29rb25haSB1dGNhIDMuMIIBIjANBgkqhkiG9w0B
          AQEFAAOCAQ8AMIIBCgKCAQEAmeF7PJ9Q8aV526x9ShxS5G5O8dOXdgYoB3XYbxFobekxT+IE5Aa0
          esTHJtpWjSwUwIiTBFVvAr7t9xjf1Rw/inUOt1b/ig24awBofxaJlzyMcIQmZy5LQJIZPovDTd5k
          IUq502nyuzIP36tva7cVJZfALImQBU+FbMSiY69JKHSa4DeUauCeY27RAg6U03bERArgfGaYqFsL
          DGaW8HVps2Fr19K02RRSx7v01fcqydg0uRiyfBU+PRvXjRC95OdPMHVPi7A7W0CeD2QpUMA0fT1Q
```

kau.gov.hu login

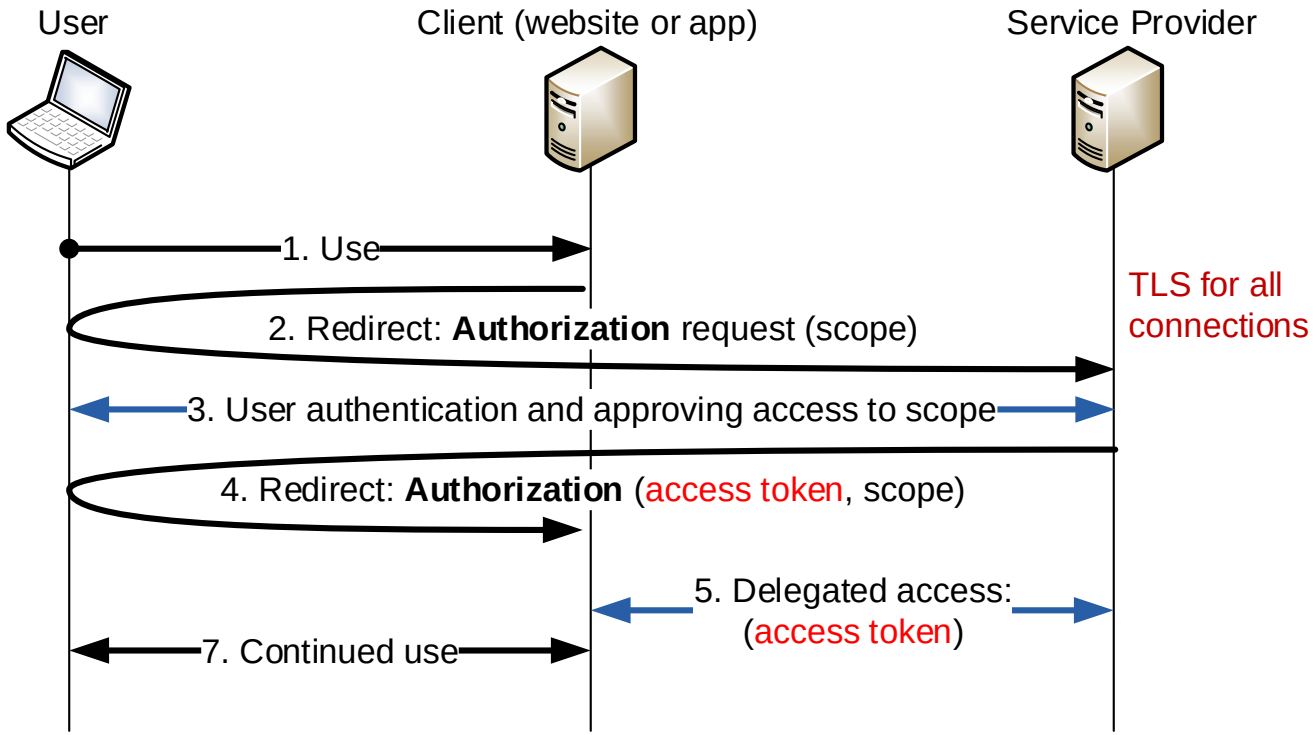
Titkosított szimmetrikus kulcs:

```
aXRlbGVzLmdvdi5odS9jcmwvR09WQ0EtTlEtU0VDLmNybDAOBgNVHQ8BAf8EBAMCBDAwEwYDVR0l
BAwwCgYIKwYBBQUHAwQwFwYDVR0RBBAwDoEMaW5mb0BuaXN6Lmh1MA0GCSqGSIb3DQEBCwUAA4IB
AQBoRCZd/jGQnBoIUL4jOo0XAJ+0SpLsG+6jUcq4+G2rsXjI5FJQUaBbm9SqxAC5PWR6QeNGx3r4
gaRH9B8YzvhYYfiR9lIapcmNc3puN6ZULmQna+1k2XSxODXvbGALzfbkIZZBXauSEsXTRxpSWCHx
E789JGD2SABKwCRWLDQLNX5c7dwpRkyPS0DBt+bi++IThA5c1glHWljiLVhJN9AAehL0kZk8n6l0
pAiN++H7UF1A0Gy9T5fGPVRc0IL3QMScbMscTO4kTkBdnW7immec1bdIZRmu1QcjU8c3tKy7Govz
h4jaWEEAyN1sgNPqyxtprr0h9CxMEp+KuSzRqMUE
      </ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
▼<xenc:CipherData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
  ▼<xenc:CipherValue>
      G0b8O9jxao01lpfZ/AapbA1CNwEqiYwKy77tByuO2dDUGD/+EirTnkEuFFShV8mcnb1s4ALYG6hnp4XRNTRvAce
    </xenc:CipherValue>
  </xenc:CipherData>
▼<xenc:ReferenceList>
    <xenc:DataReference URI="#_ea58bcbe55e27d99c65cea3b60314105"/>
  </xenc:ReferenceList>
</xenc:EncryptedKey>
```

OAuth 2.0

- OAuth was designed for authorization (i.e. delegation)
  - Allow an external web site or app to access a service on the user's behalf
- Examples:
  - Authorize an external web site or app to update your Facebook profile or page
- Standardized by IETF (RFC 6749, RFC 6750)
  - Many implementation options cause interoperability issues
  - OAuth 2.0 security is based only on TLS (Oath 1.0 used client signatures)

OAuth 2.0 protocol



- User authorizes the client (web site or mobile app) to access the service
  - Client may restrict the scope of delegated access
- Security based on an opaque access token and TLS
  - Token is typically a random number
  - Service providers remembers the scope of authorized access for each token

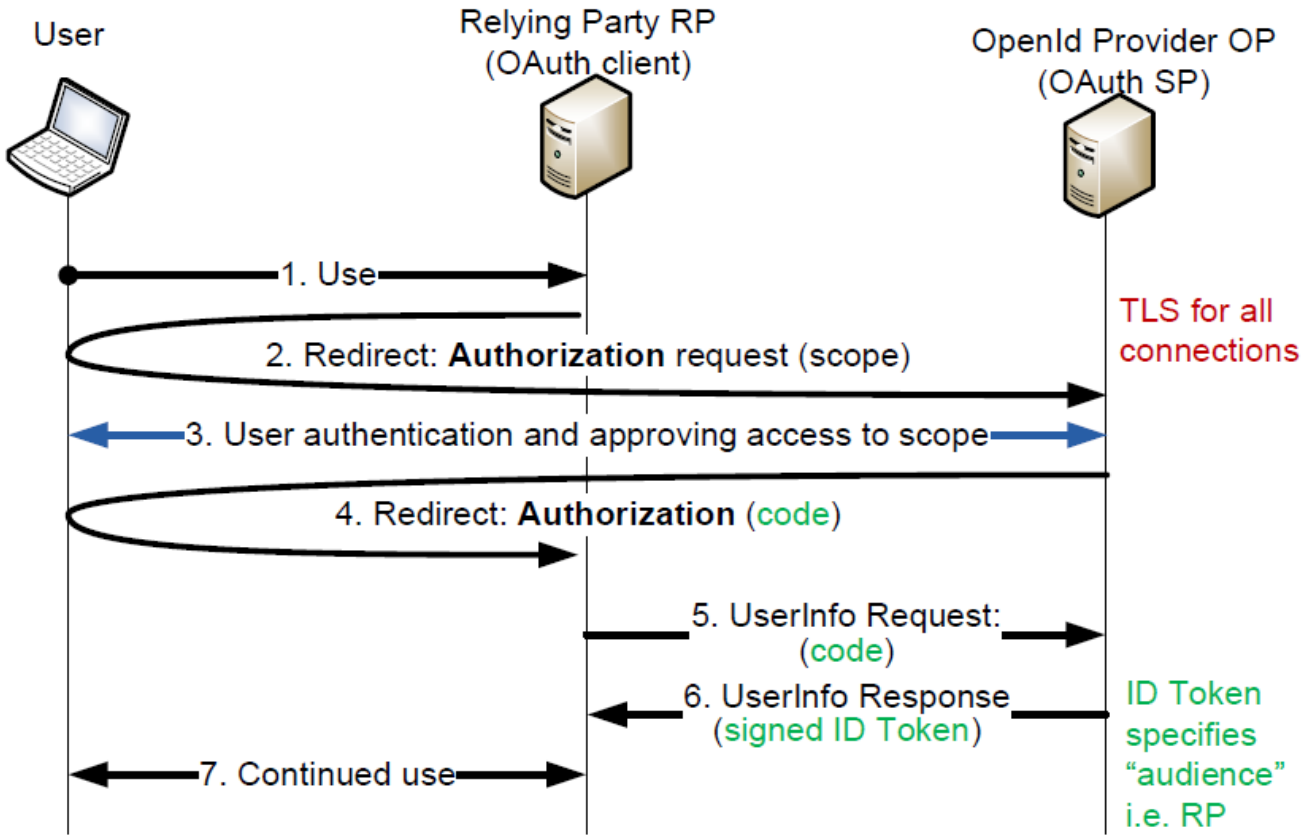
OAuth for authentication?

- The message flow in OAuth looks like SAML → tempting to use the same protocol for authentication
  - User would prove its identity by delegating access to a (dummy) resource associated with the user account
- In principle, this is a bad idea:
  - OAuth access token enables client to access a resource on the service provider
  - The client in OAuth does not know or care who gives it the token, as long as the token works for accessing SP
  - The protocol does not prevent the client from sharing the token with others

  ➔ Malicious client can impersonate its users to other clients
- Autentication based on OAuth standardized as OpenId Connect

  http://openid.net/developers/specs/

OpenId Connect



- Authentication built on OAuth 2.0, REST API, JSON data formats
- Access token is replaced with a code that is used only for retrieving user identity and other attributes from OP

ID token encoding

```
{
   "iss"        : "https://c2id.com",
   "sub"        : "alice",
   "aud"        : "s6BhdRkqt3",
   "nonce"      : "n-0S6_WzA2Mj",
   "exp"        : 1311281970,
   "iat"        : 1311280970,
   "auth_time"  : 1311280969,
   "acr"        : "urn:2fa",
   "at_hash"    : "MTI..."
 }
```

- Encoded as a JSON Web Token (JWT).
- The claims about the subject are packed in a simple JSON object.
- It is signed. Typically with the provider's private RSA key or a shared secret (HMAC) issued to the client during registration.
- Is URL-safe.