Polymorphic Encryption and Pseudonymization in the Dutch eID scheme

Eric.Verheul@logius.nl

IRMA meeting, 23 September 2016

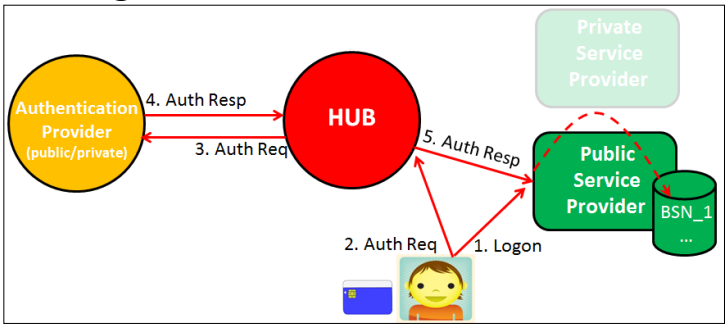
1

Agenda

- Background on the Dutch eID scheme
- The Dutch eID Introduction Plateau
- Limitations of the Dutch eID Introduction Plateau
- Dutch eID scheme based on Polymorphic Pseudonymization
- Polymorphic Pseudonyms on the Dutch ID card (PPCA)
- Conclusion

2

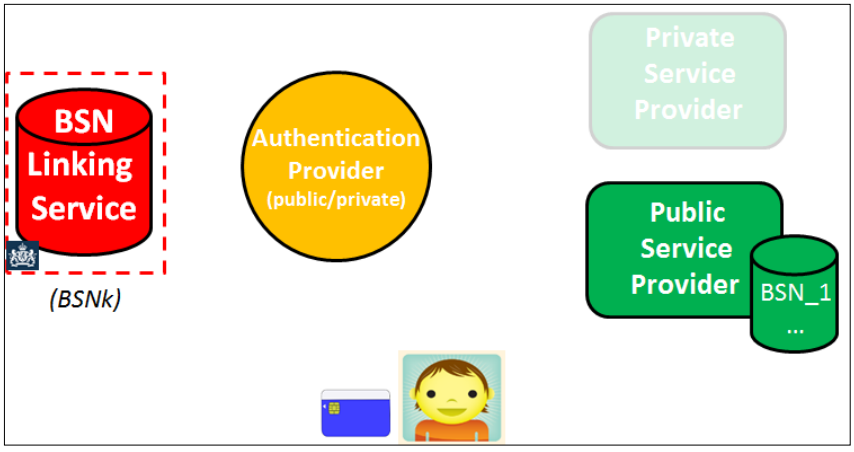
Background on the Dutch eID scheme



- The Dutch eID scheme is a *Hub-and-spoke* **federation** based on SAMLv2.
- Striving for optimal synergy with private authentication providers.
- As Dutch government services are based on the Dutch Social Security Number (**BSN**), this needs to be communicated by APs to public SPs.
- Leaving out HUB for simplicity of presentation.
- Details on https://afsprakenstelsel.etoegang.nl

3

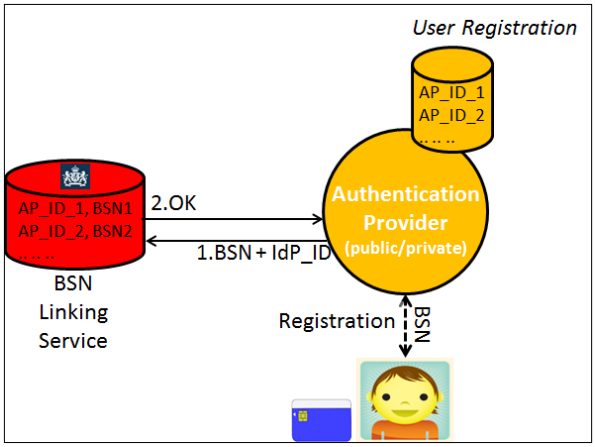
The Dutch eID Introduction Plateau



- First pilots using private APs to authenticate citizens to government.
- BSN Linking Service (BLS) facilitates BSN provisioning to public SPs.
- Two BLS use cases: Registration and Usage.

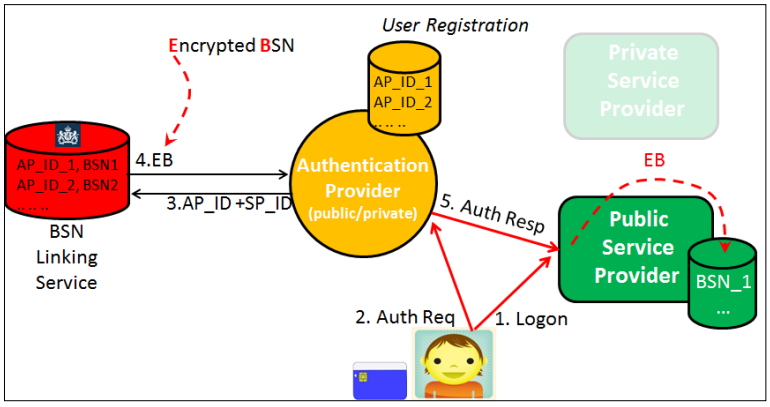
4

The Dutch eID Introduction Plateau: Registration



- During Registration user's BSN is registered at BLS under local AP identifier (AP_ID)
- AP_ID is linked by AP with the authentication means of the user
- BSN to be deleted by AP after user registration

The Dutch eID Introduction Plateau: Usage



- AP looks up local AP identifier of user after successful authentication.
- AP sends local AP identifier and SP name to BLS.
- BLS looks up BSN and SAML (RSA) encrypts this with public key of intended service provider. This results in EB.
- Intended service provider decrypts EB and retrieves BSN.

Limitations of the Dutch eID Introduction Plateau

- Several Security and Privacy Impact Assessments (PIAs) were performed on the Introduction Plateau. See http://idensys.nl.
- Several risks identified that need to be structurally addressed, e.g.:

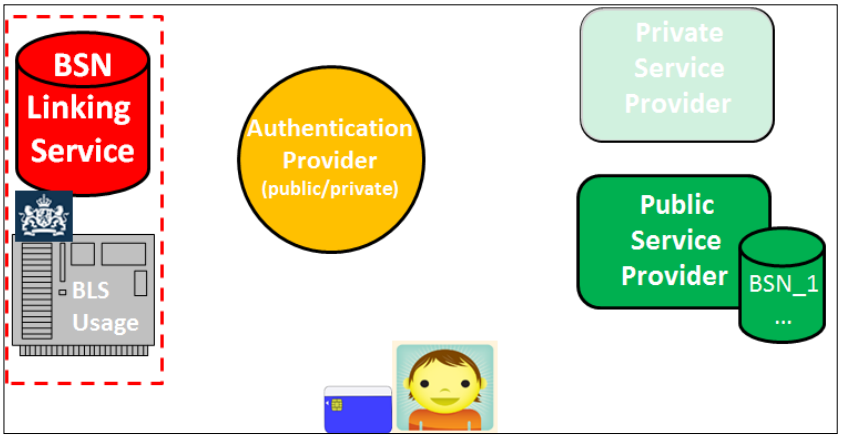
#	
1.	Both BLS and APs are hotspots: both can follow citizen movements. This is not desirable for e.g. health care applications. (*)
2.	No centralized mechanism for users to assess where they have registered identification means. This frustrates fraud detection.
3.	BLS is Single Point of Failure (SPOF)

- Polymorphic Pseudonymization designed in 2014 as privacy enhancing technology in the Dutch federative eID scheme.
- Full details on http://idensys.nl. See also https://eprint.iacr.org/2015/1228.

(*) Making the AP 'blind', i.e. not letting him know the intended SP, disables AP protection of user against fraud, cf. Man-in-the-Browser attacks.

7

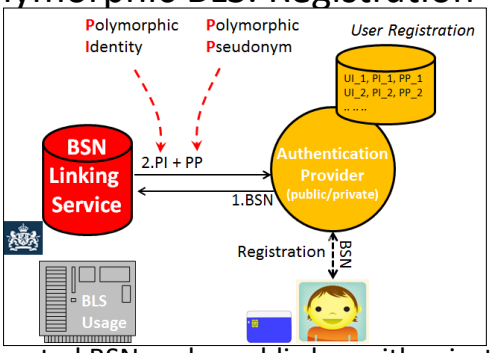
Dutch eID scheme based on polymorphic pseudonymization



- BSN Linking Service is split into two services: Registration and Usage.

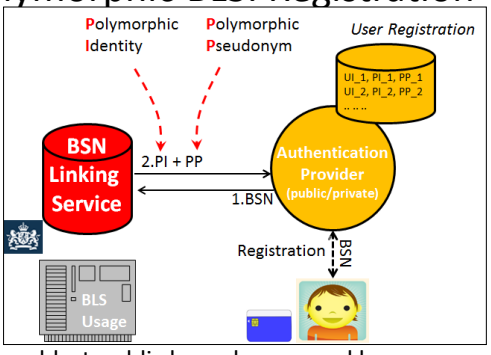
8

Polymorphic BLS: Registration



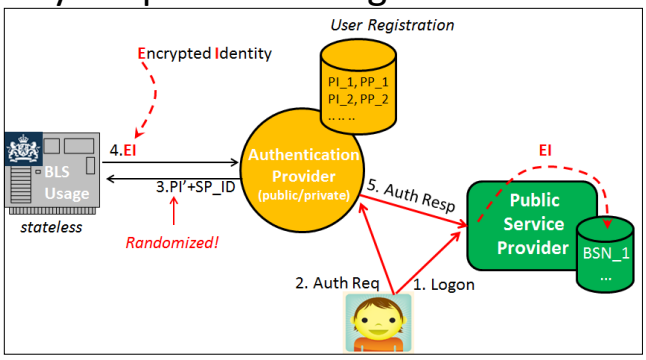
- PI is ElGamal encrypted BSN under public key with private key only known by Key Management Centre.
- PP is ElGamal encrypted HMAC value of BSN under public key with private key only known by Key Management Centre.
- PI and PP are AP specific (not AP interchangable)
- PI/PP linked with user at AP
- BSN to be deleted by AP after registration

Polymorphic BLS: Registration



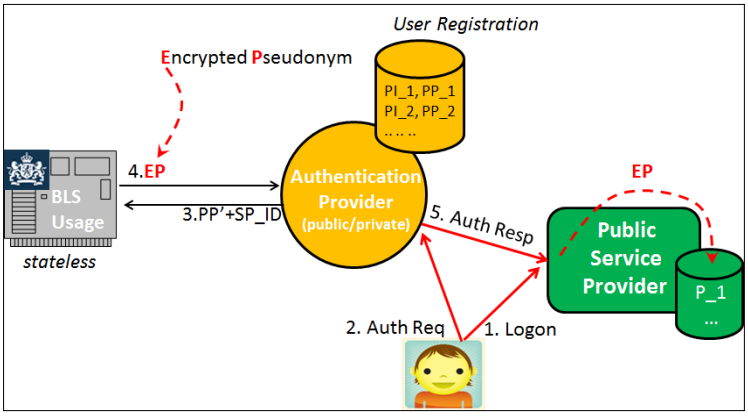
- ElGamal is one of the oldest public key schemes and has very convenient *homomorphic* properties, e.g.:
  - A central party can transform an encrypted message under public key to another public key of an intended party without getting knowledge of the message (*Re-Keying*).
  - A central party can also transform the contents of an encrypted message without knowing the end-result inside (*Re-Shuffling*).
  - ElGamal cryptograms are self-randomizable (make unlinkable copies).

Polymorphic SLS: Usage for identities



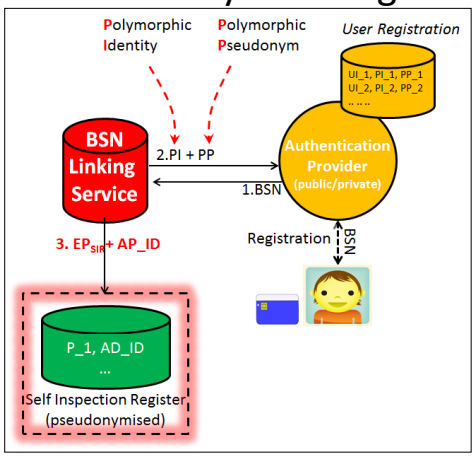
- AP looks up PI of user after successful authentication.
- AP sends randomized PI (PI') and SP name to SLS Usage service.
- BLS Usage transforms PI' to Encrypted BSN for intended SP (Re-key).
- Intended service provider decrypts EI and retrieves BSN
- BSN not accessible for AP from EI.
- BLS Usage service is stateless and no longer hotspot (but AP still is)

Polymorphic SLS: Usage for pseudonyms



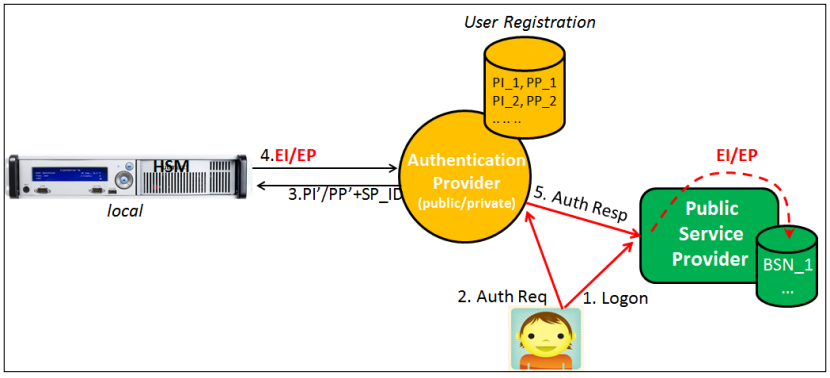
- Similar setup allows for providing pseudonyms instead of identities.
- Pseudonyms are Service Provider specific.
- Pseudonyms are compatible: all APs will deliver same pseudonym to SP.
- Pseudonyms at service provider are unknown by AP.

User access to where they have registered id means



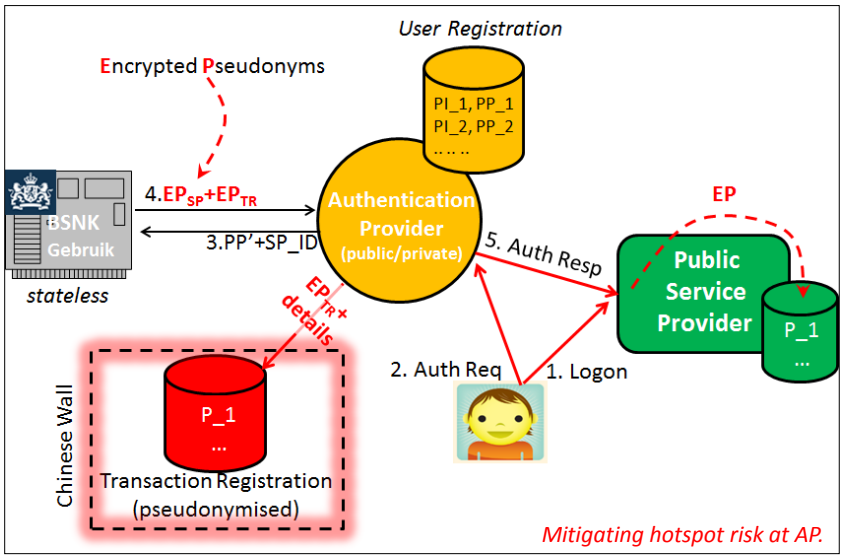
- During registration Self Inspection Register (SIR) is sent message
- SIR is just a service provider, based on pseudonyms
- Users can have access to SIR through any registered identification means
- Allows for easy self checking by users

Optional usage of Hardware Security Modules



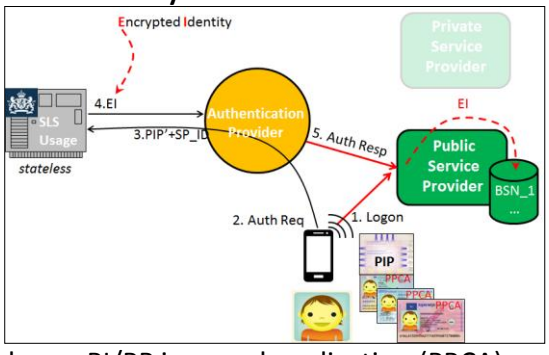
- By placing the BLS transformation keys in a Hardware Security Module (HSM) one can provide the BLS Usage functionality locally at AP
- This takes away the SPOF at BLS, but also has other security advantages

Optional separation of user- and transaction data at AP



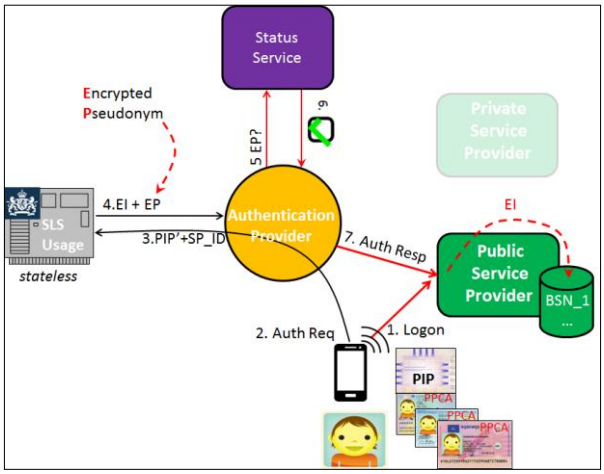
15

Polymorphic Pseudonyms on the Dutch ID card (PPCA)



- One can also place a PI/PP in a card application (PPCA), e.g. on national ID card, and let AP read it like a fingerprint (PACE/TA/CA)
- PPCA sends randomized PI and/or PP to AP. This amounts to three ECC multiplications and additions. This is conveniently supported in recent Javacard extensions (3.0.5) meant for PACE.
- In effect we get a federated implementation of the German eID card.

Polymorphic Pseudonyms on the Dutch ID card (PPCA)



- Encrypted Pseudonym setup also allows for implementation of a central pseudonymous eIDAS Status Service. This is an alternative for the rather complex black- and whitelisting in the German eID concept.

Conclusion

#	
1	Both BLS and APs are hotspots: both can follow citizen movements. This is not desirable for e.g. health care applications. (*)
2	No centralized mechanism for users to assess where they have registered identification means. This frustrates fraud detection.
3	BLS is Single Point of Failure (SPOF)

Pending Privacy Impact Assessment.

Conclusion

- Recently Market Consultation was concluded on Dutch eID applet and middleware which included questions on polymorphic support.
- A Proof-of-Concept is planned for this autumn with the described polymorphic BLS.
- Requirements for HSMs at polymorphic Authentication Providers are compiled. Procurement process started.
- No irreversible steps without explicit consent of Dutch parliament!