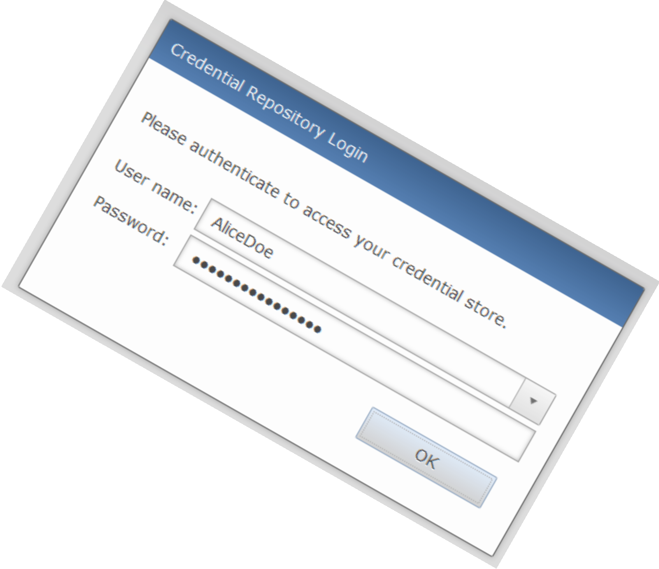
WP8 Combined Demo on

IDM GE (NSN)
Data Handling GE (SAP)
Privacy GE (IBM)

Sept. 29th 2014, v8

Overview



Credential Repository Login

Please authenticate to access your credential store.

User name: AliceDoe

Password: •••••••••••••••

- Description of the Use Case
- High Level Architecture
- Prerequisites
- Message Flow
- Implementation Details
- Interfaces
- Development Tasks with Status
- Limitations
- Benefits of the Demonstrator
- Differences to the ABC4Trust Project
- Documentation
- Additional Links

DESCRIPTION OF THE USE CASE

- A file storage service (e.g. File Store) will be enhanced with the Data Handling GE and allow access to its resources if the user can satisfy the policies attached to these resources.

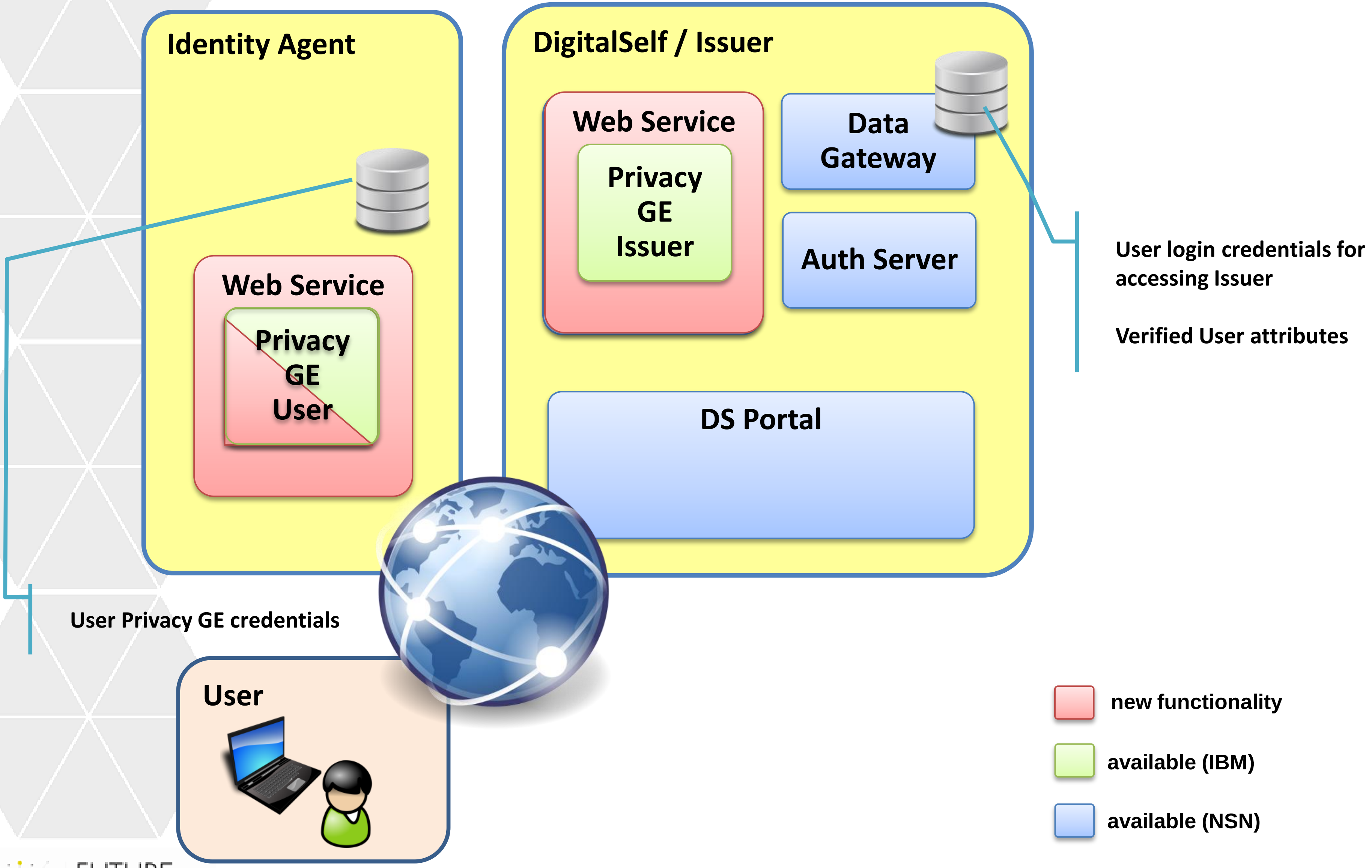
- With the Privacy GE, users are in full control of which attributes they reveal when interacting with the File Store. The Privacy GE is distributed over 3 sites: the ‘User in the Cloud’, the ‘Verifier as a Service’ and the ‘Issuer Service’.

- The ‘Verifier as a Service’ connects to the File Store thereby enhancing it with Privacy GE features.

- The ‘Issuer Service’ is integrated into the IDM GE.

While respecting privacy of the user, selective attribute sharing will be supported restricted to the ‘need to know’ principle.

HIGH LEVEL ARCHITECTURE: *ENROLMENT*



Identity Agent

Web Service

Privacy GE User

DigitalSelf / Issuer

Web Service

Privacy GE Issuer

Data Gateway

Auth Server

DS Portal

User login credentials for accessing Issuer

Verified User attributes

User Privacy GE credentials

User

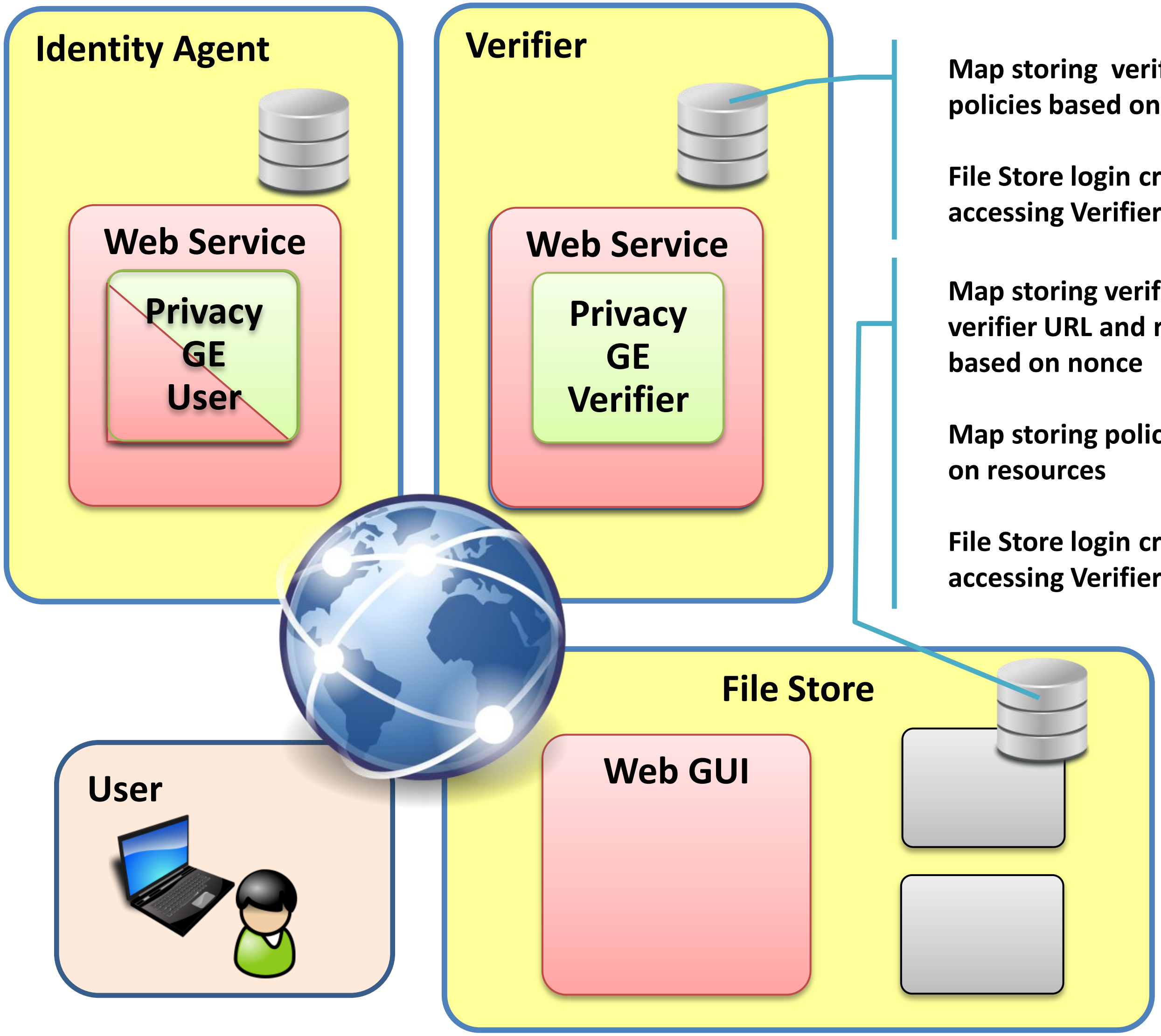
🟥 new functionality

🟩 available (IBM)

🟦 available (NSN)

HIGH LEVEL ARCHITECTURE: *USE-CASE*

“anonymous access of resources”



Identity Agent

Web Service

Privacy GE User

Verifier

Web Service

Privacy GE Verifier

User

File Store

Web GUI

Map storing verification policies based on policy ID

File Store login credential for accessing Verifier

Map storing verification policy, verifier URL and resource URL based on nonce

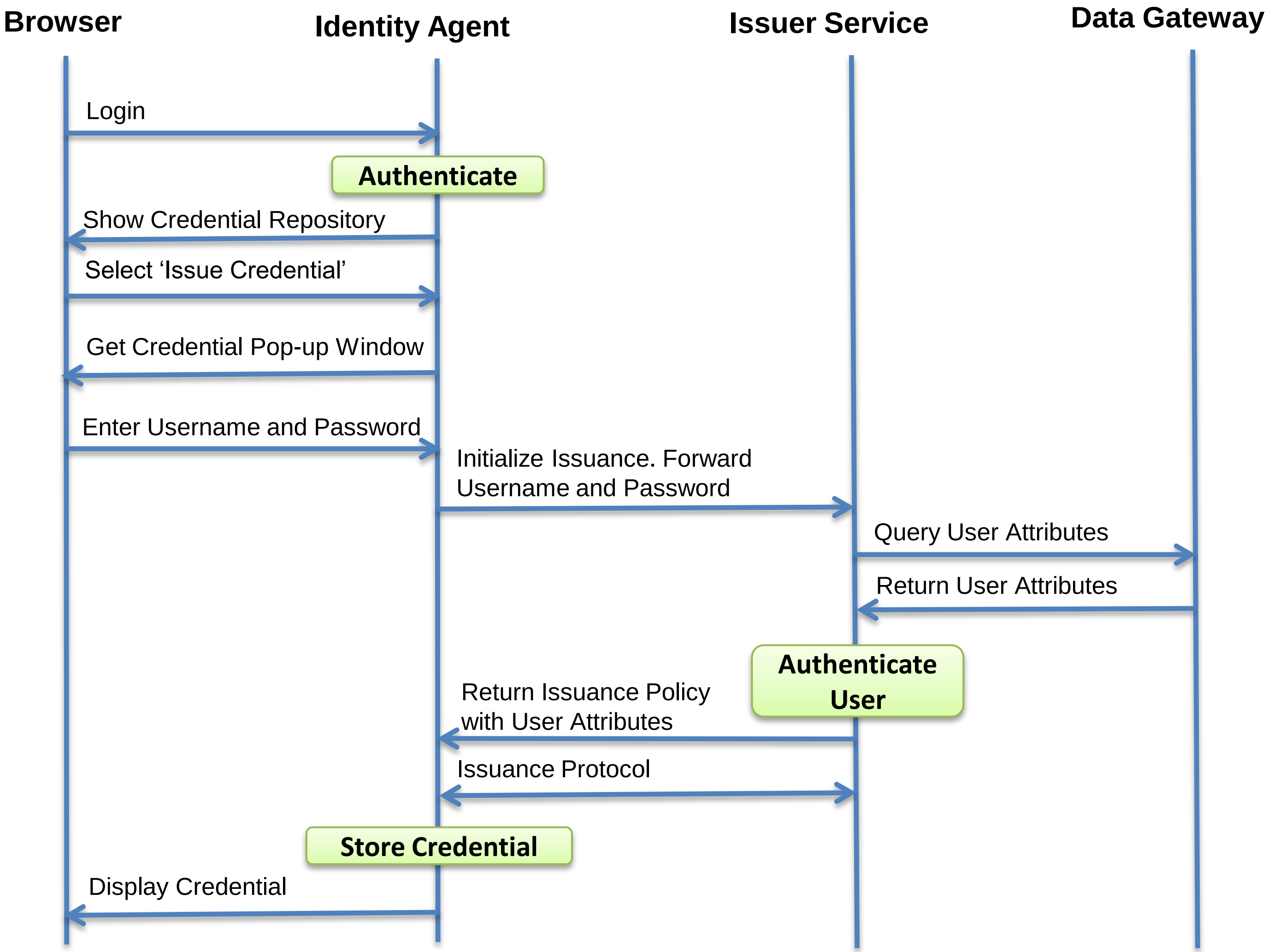
Map storing policy IDs based on resources

File Store login credential for accessing Verifier

🟥	new functionality
🟩	available (IBM)
⬜	available (SAP)

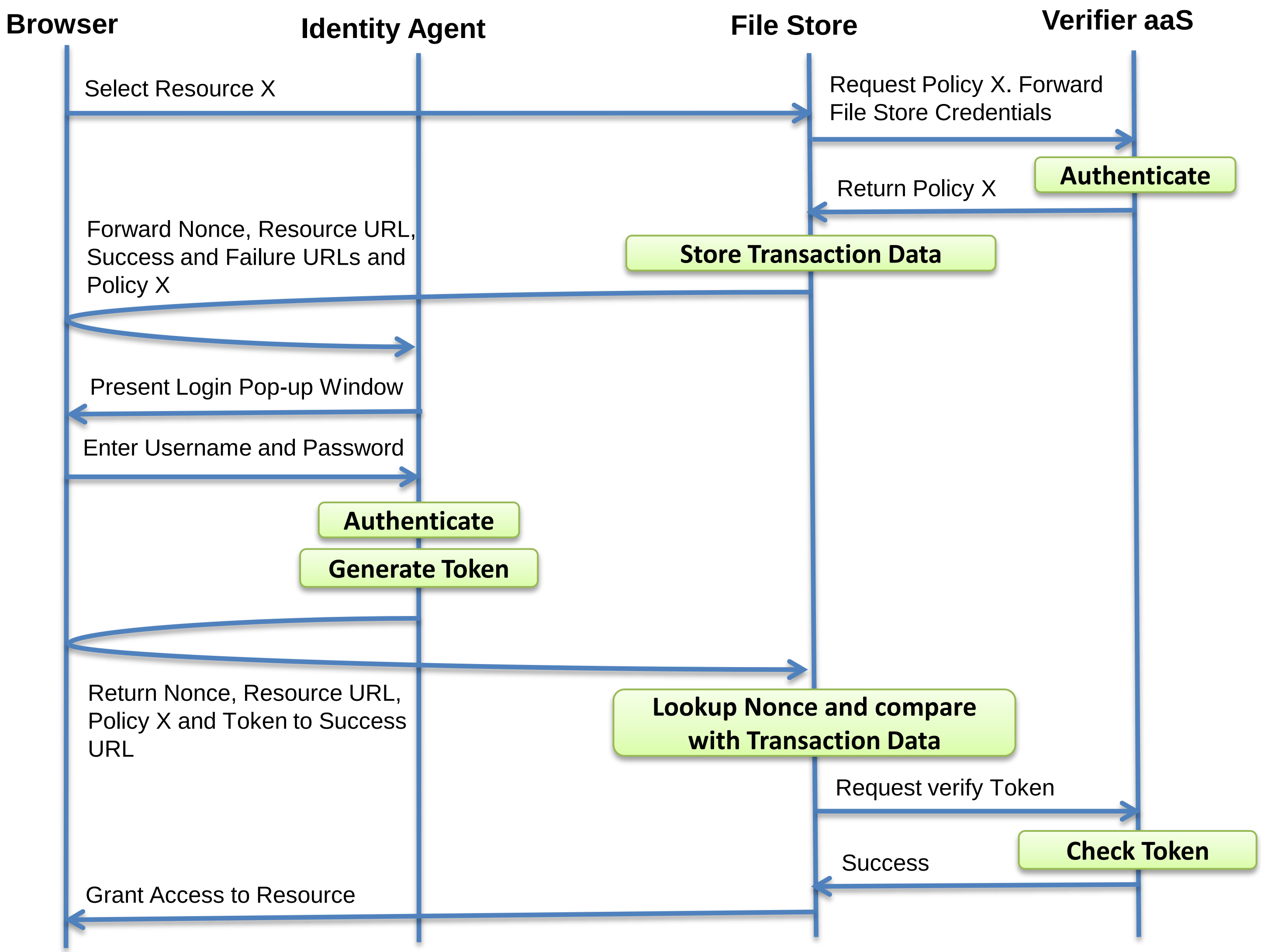
FUTURE INTERNET PPP

MESSAGE FLOW (ENROLMENT)



Browser
Identity Agent
Issuer Service
Data Gateway
Login
Authenticate
Show Credential Repository
Select ‘Issue Credential’
Get Credential Pop-up Window
Enter Username and Password
Initialize Issuance. Forward Username and Password
Query User Attributes
Return User Attributes
Authenticate User
Return Issuance Policy with User Attributes
Issuance Protocol
Store Credential
Display Credential

MESSAGE FLOW (USE-CASE)


Browser
Identity Agent
File Store
Verifier aaS
Select Resource X
Request Policy X. Forward File Store Credentials
Authenticate
Return Policy X
Store Transaction Data
Forward Nonce, Resource URL, Success and Failure URLs and Policy X
Present Login Pop-up Window
Enter Username and Password
Authenticate
Generate Token
Return Nonce, Resource URL, Policy X and Token to Success URL
Lookup Nonce and compare with Transaction Data
Request verify Token
Check Token
Success
Grant Access to Resource

PREREQUISITES

- The File Store service has stored resources which can only be accessed by users satisfying the policies attached to them

- The IDM GE has stored verified attribute values of the user including her login password for accessing the Issuer Service. The FI-WARE relevant attribute values are predestined for generating a Privacy GE credential

IMPLEMENTATION DETAILS I

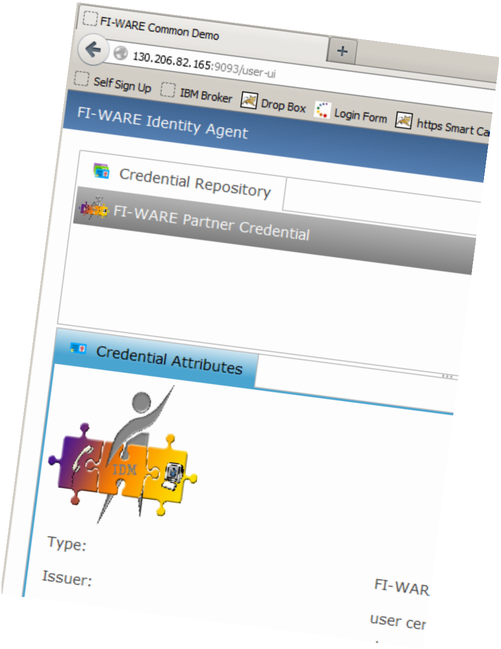
- The File Store service will be enhanced to show a list of resources without requiring a preceding login
- The user can choose a specific resource she wishes to access
- The user can choose the Identity Agent which must generate the token
- When the user selects a specific resource with a specific policy ID, the File Store fetches the presentation policy from the Verifier aaS
- An ‘auto submit form’ will make the user generate an HTTP-POST and send it to the Identity Agent
- The auto submit form embedded in the GUI of the File Store contains
  - a nonce (generated by and stored in the File Store)
  - the presentation policy received from the Verifier aaS
  - the URL of the requested resource
  - a failed and a success URL of the File Store
- The File Store stores the ‘transaction data’ using the nonce as handle in its database

IMPLEMENTATION DETAILS II

- After logging in to the Identity Agent, this service generates a presentation token on behalf of the user
- An auto submit form will make the user generate an HTTP-POST and send it to the File Store
- The auto submit form embedded in the GUI of the Identity Agent contains
  - the nonce
  - the URL of the requested resource
  - the presentation policy
  - the presentation token
- The File Store will then
  - fetch the ‘transaction data’ (presentation policy and resource URL) using the nonce as handle
  - compare the received policy with the stored policy
  - compare the received resource URL and the stored resource URL
  - forward the presentation policy and the presentation token to the Verifier aaS

IMPLEMENTATION DETAILS III

- The Verifier aaS will check the token
- If the token is ok, the File Store will finally grant access to the requested resource and delete the ‘transaction data’ including the nonce from its database



FI-WARE Common Demo

130.206.82.165:9093/user-ui

FI-WARE Identity Agent

Credential Repository

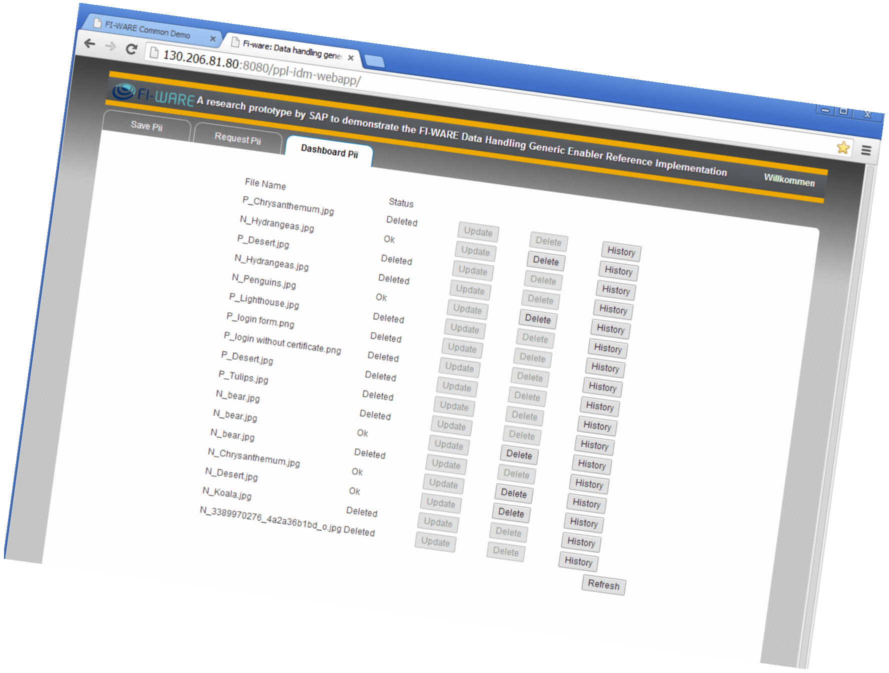
FI-WARE Partner Credential

Credential Attributes

Type:

Issuer: FI-WAR

user cer



FI-WARE Common Demo

Fi-ware: Data handling gene

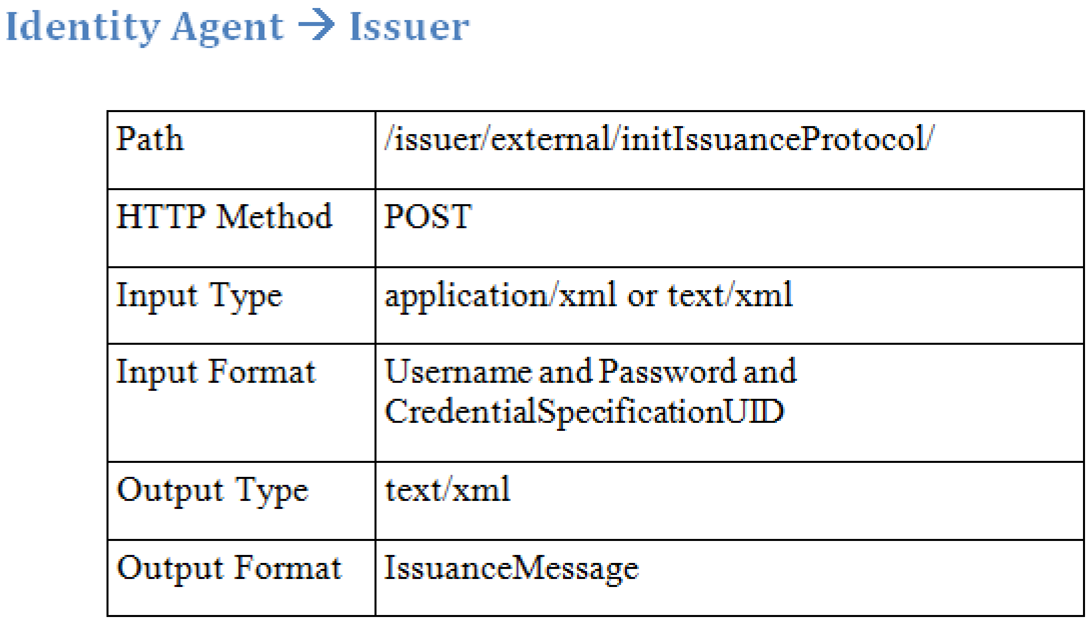
130.206.81.80:8080/ppl-idm-webapp/

FI-WARE A research prototype by SAP to demonstrate the FI-WARE Data Handling Generic Enabler Reference Implementation

Willkommen

File Name	Status
P_Chrysanthemum.jpg	Deleted
N_Hydrangeas.jpg	Ok
P_Desert.jpg	Deleted
N_Hydrangeas.jpg	Deleted
N_Penguins.jpg	Ok
P_Lighthouse.jpg	Deleted
P_login form.png	Deleted
P_login without certificate.png	Deleted
P_Desert.jpg	Deleted
P_Tulips.jpg	Deleted
N_bear.jpg	Deleted
N_bear.jpg	Ok
N_bear.jpg	Deleted
N_Chrysanthemum.jpg	Ok
N_Desert.jpg	Ok
N_Koala.jpg	Deleted
N_3389970276_4a2a36b1bd_o.jpg	Deleted

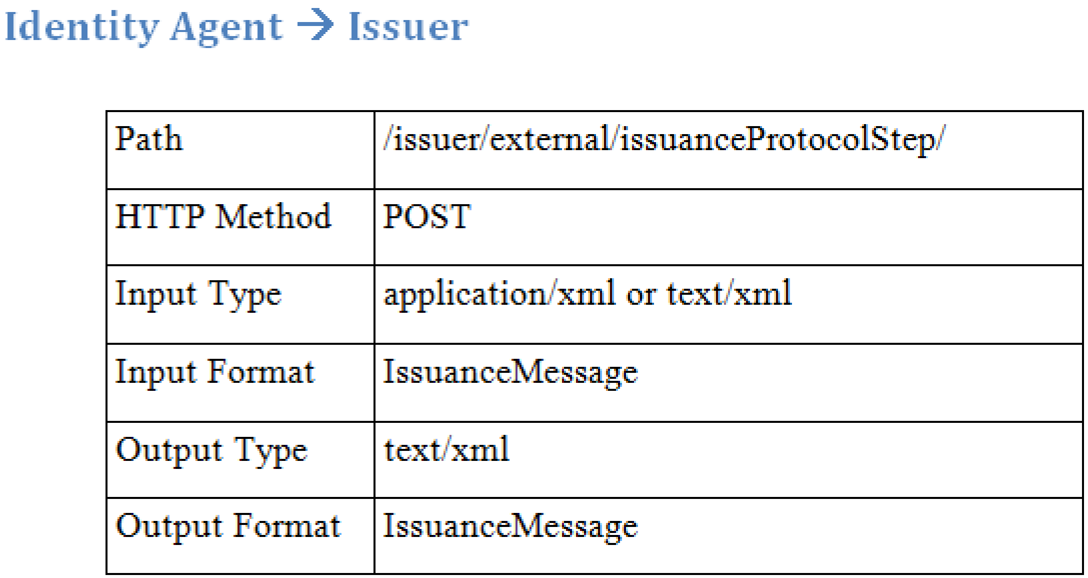
INTERFACES I



Identity Agent → Issuer

Path	/issuer/external/initIssuanceProtocol/
HTTP Method	POST
Input Type	application/xml or text/xml
Input Format	Username and Password and CredentialSpecificationUID
Output Type	text/xml
Output Format	IssuanceMessage

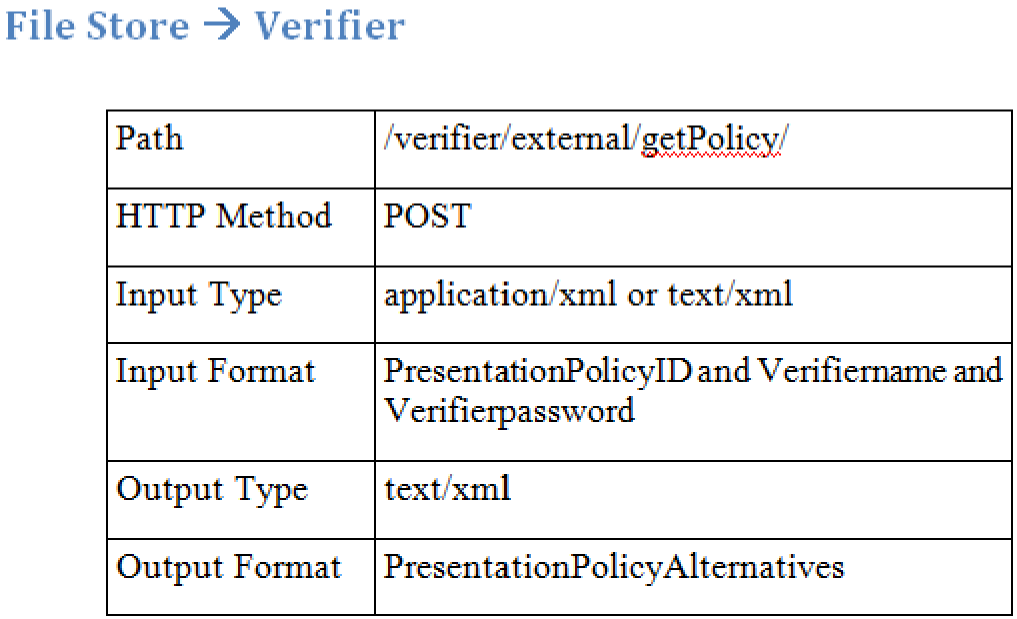
INTERFACES II



Identity Agent → Issuer

Path	/issuer/external/issuanceProtocolStep/
HTTP Method	POST
Input Type	application/xml or text/xml
Input Format	IssuanceMessage
Output Type	text/xml
Output Format	IssuanceMessage

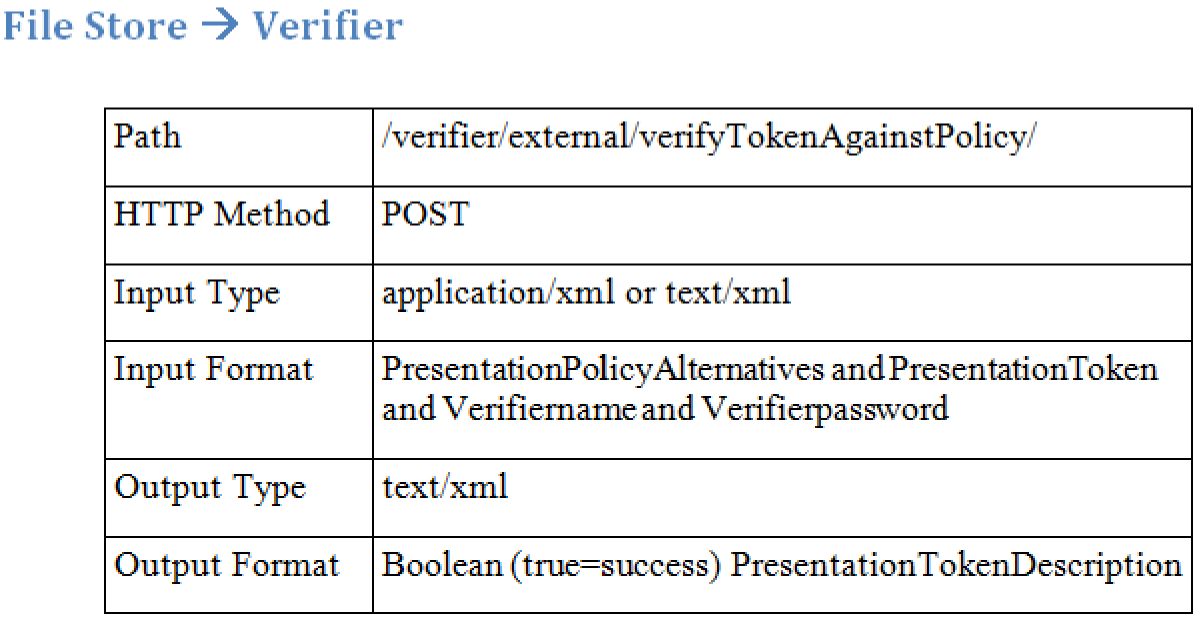
INTERFACES III



File Store → Verifier

Path	/verifier/external/getPolicy/
HTTP Method	POST
Input Type	application/xml or text/xml
Input Format	PresentationPolicyID and Verifiername and Verifierpassword
Output Type	text/xml
Output Format	PresentationPolicyAlternatives

INTERFACES IV



File Store → Verifier

Path	/verifier/external/verifyTokenAgainstPolicy/
HTTP Method	POST
Input Type	application/xml or text/xml
Input Format	PresentationPolicyAlternatives and PresentationToken and Verifiername and Verifierpassword
Output Type	text/xml
Output Format	Boolean (true=success) PresentationTokenDescription

fi-ware

DEVELOPMENT TASKS WITH STATUS

- (IBM) Identity Agent
  - ✓ Modified graphical identity selection user interface such that it can run as a web-based cloud service where users are authenticated
  - ✓ Added a credential issuance wizard to the Identity Agent that triggers a credential issuance protocol with an issuer service
  - ✓ Trigger the generation of a presentation token upon reception of a presentation policy and forward the user to the provided success/failure URL
  - ▪ Future extension: allow users to select which credentials shall be the basis for the token generation, instead of simply selecting the first possible choice

- (NSN) Issuer Service
  - ✓ Provide RESTful interfaces to the methods of this service
  - ✓ Authenticate users requesting issuance
  - ✓ Enhance the database to allow storage of new attributes
  - ✓ Enhance the SelfSignUp application to allow administration of new user accounts

- (NSN) Verifier as a Service
  - ✓ Provide RESTful interfaces to the methods of this service
  - ✓ Authenticate services requesting verification
  - ✓ Provide pre-defined XML presentation policies files

FUTURE
INTERNET
PPP

DEVELOPMENT TASKS WITH STATUS

- (SAP) File Store
  - Provide a UI for the File Store Service
    - Provide an interface for storing the resources and attaching policies to them
    - Provide an interface for retrieving the resources without logging in
- (NSN) Example Applications
  - ✓ Develop an Example Drop Box and an Example Broker as feasibility study to verify the chosen interfaces between these entities
  - ✓ Develop an Example Issuer
- (ALL) Perform Integration Tests
  - ✓ Test the system with the Example Drop Box
  - Test the final system using SAP’s File Store

LIMITATIONS

- Use of pre-defined attributes/policies only
  - gender=male
  - gender=female
  - age>65
  - age>18
  - nationality=German
  - nationality=Swiss
  - nationality=French
  - companyName=SAP
  - companyName=IBM
  - companyName=NSN

- Uploading resources to the ‘File Store’ requires authentication of the users and is therefore out of scope of this demo

Benefits of the Demo

- Developing a demonstrator which can be presented inside FI-WARE and as well outside (e.g. Use Case Projects) in order to advertise the following Generic Enablers:
  - IDM GE
  - Data Handling GE
  - Privacy GE

- Prove interworking/combination of Security Generic Enablers

- Propose an easy and clear use case scenario understandable for non-experts

Differences to the ABC4Trust Project I

- ABC4Trust: The user stores her credential(s) on the smart card. The user application is installed on the user's PC.
  FI-WARE: The user application is shifted to the cloud and hosted by the 'Identity Agent'. Smart cards are not used.

- ABC4Trust: The issuer is connected to the One-IDM via WSDL and has no access to the IDM LDAP data base. The IDM Portal acts as proxy between user and issuer.
  FI-WARE: The issuer has direct access to the Digital Self 'Data Gateway'. The identity agent has direct access to the issuer via RESTful interfaces.

Differences to the ABC4Trust Project II

- ABC4Trust: The RESTful interfaces are unprotected
  FI-WARE: The RESTful interfaces have been enhanced to carry authentication credentials

- ABC4Trust: Requires Firefox or Internet Explorer
  FI-WARE: Requires Google Chrome

- ABC4Trust: Deploys Idemix and U-Prove crypto engines
  FI-WARE: Deploys only the Idemix crypto engine

➢ The two use-cases of the ABC4Trust pilots are significantly different this combined demo which integrates SAPs asset PPL into a File Store

DOCUMENTATION

Use Google Chrome as browser

In order to start the demo, select the ‘Request Pii’ tab of this URL:

http://idmlab02.extranet.nokiasiemensnetworks.com:443/ppl-webapp/

Video Clips showing the Demo can be found here:

http://idmlab03.extranet.nokiasiemensnetworks.com/fiware-open/combinedDemo/Videos/

How to operate the Demo:

http://idmlab03.extranet.nokiasiemensnetworks.com/fiware-open/combinedDemo/Docs/Cookbook%20for%20testing%20the%20combined%20demo.pdf

Source Code and Libraries:

http://idmlab03.extranet.nokiasiemensnetworks.com/fiware-open/combinedDemo/Code/

ADDITIONAL LINKS I

NSN Registration Tool for adding a IDM GE (One-IDM) account.

(The attributes of this account will be used for generating the Privacy-ABC credentials)

http://idmlab02.extranet.nokiasiemensnetworks.com:444/SignUp/

IBM Identity Agent

http://130.206.81.92:9093/user-ui

NSN Example Drop Box:

http://idmlab07.extranet.nokiasiemensnetworks.com:443/ExampleDropBox/

ADDITIONAL LINKS II

NSN Example Identity Broker

http://idmlab02.extranet.nokiasiemensnetworks.com:443/ExampleBroker/

Issuer Database check URL:

http://idmlab06.extranet.nokiasiemensnetworks.com:443/issuer_aas/issuer/generic

NSN Example Issuer without IDM Database:

http://idmlab02.extranet.nokiasiemensnetworks.com:443/ExampleIssuer/issuer/external/initIssuanceProtocol

http://idmlab02.extranet.nokiasiemensnetworks.com:443/ExampleIssuer/issuer/external/issuanceProtocolStep

THANK YOU!

NOKIA

SAP

IBM

THALES

orange™

Atos

INRIA

T

FUTURE
INTERNET
PPP