Network Initiated USSD-based Authenticator

Modrna WG meeting

Dawid Wroblewski, IDG Chair,

Network Initiated USSD-based Authenticator - Procedure

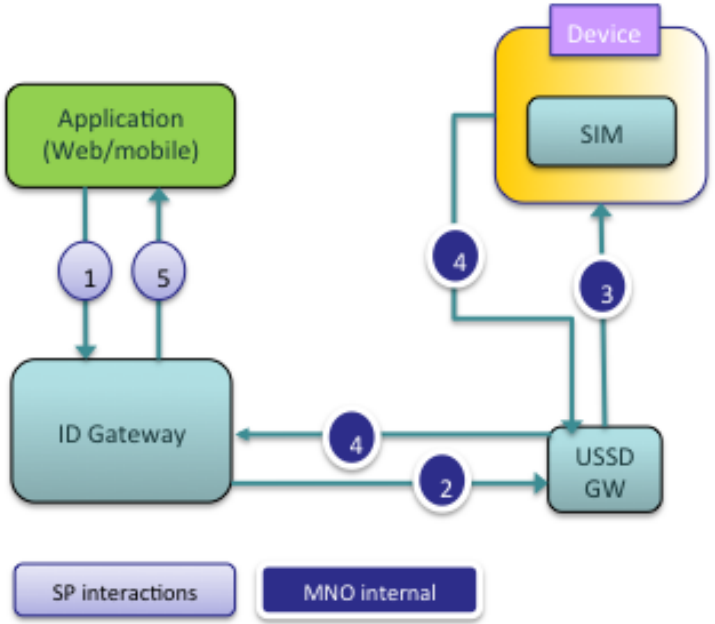
1. The application (desktop, tablet or mobile phone) calls an OIDC Authorisation towards the mobile operator ID GW to authenticate the user.

2. The mobile operator ID GW interacts with the USSD GW to send USSD messages.

3. The USSD GW sends a message to the device.
4. For LoA3, the device pops up a USSD menu to type the PIN. For seamless login, this can simply type 1 to authorise and 0 to cancel, if 1FA is sufficient.

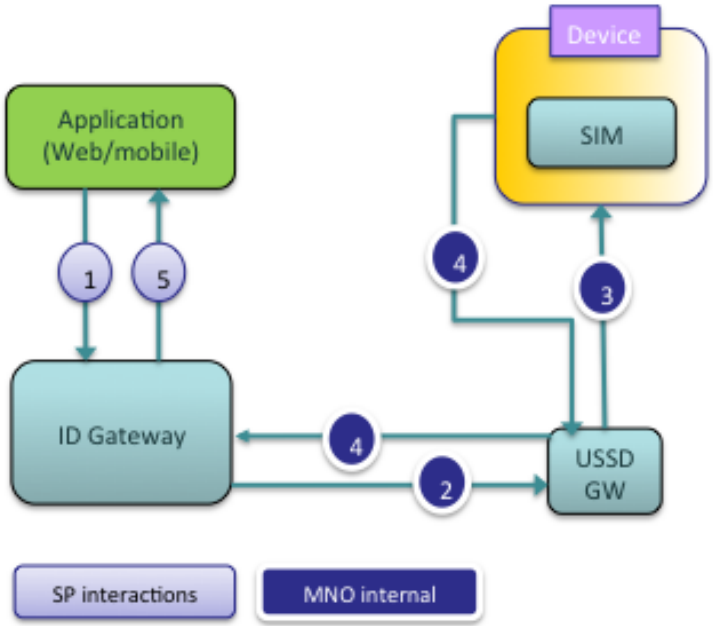
5. The USSD message is sent back to the ID GW, through the USSD GW.

6. The ID GW service responds to the application.



Source IDG.09 v1.1 Published 12 May 2017

Network Initiated USSD-based Authenticator - Security



1. USSD is plain text and presumably cannot be easily hashed as there is no device-side application.
2. However, in theory USSD cannot be easily intercepted (man-in-the-middle attacks would entail significant effort and equipment)
3. It would work for the Click OK service (LoA1) and possibly also for the Enter PIN variant (LoA3).

This mechanism would support both the Click OK and the Enter PIN authentication modes (user's PIN being validated by the ID GW).

Network Initiated USSD-based Authenticator – Pros and Cons

Pros	Cons
It uses the mobile operator assets.	Minimal user experience.
It is not dependent on a data channel, it works on the signalling plane.	Might not work on some types of network generations (4G/5G)
It works in roaming conditions, across devices.	Inconsistent UX/UI (based on how USSD messages are handled by device)
It potentially supports both LoA2 and LoA3.	Transmission security possibly not secure enough for LoA3.

Security Fraud and Risk Assessment - Feedback

Pros	Cons
USSD messages can only be sent by the mobile operator systems (ID GW) and not by other entities.	Potentially standard imposter attack (imposter uses own phone/own PIN) if the initial ID and entered MSISDN are not coupled within the system (why does it ask user to enter MSISDN if it is coupled?). If this is not the case then SIM Swap could be an issue.

SFRA Recommendations on Mitigations

Augment MSISDN as user ID by another element requested from the user, which is captured during user registration (e.g. a spam code or DOB) or based on the context (e.g. model of the phone or location) depending on the implementation.