H. Roßnagel, C.H. Schunck, J. Günther (Hrsg.): Open Identity Summit 2023,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2017 141

Electronic identity mass compromize: Options for recovery

Lothar Fritsch[1]

Abstract: *A National Digital Identity Framework should be designed in a proactive manner, should focus on a resilience-oriented approach, and should be aimed at limiting the risks that may originate from identity data management [IT18].* What is the preparedness of digital identity providers for recovery from compromise that affects large numbers of identities? Failures or attacks may destroy authenticators, data or trust chains that are the foundations of large identity ecosystems. The re-issuance of digital identities, of authenticators or the re-enrollment of the user base should get planned as contingency measures. Important parameters will be recovery time, complexity of re-registering subjects, distribution of effort between certification authorities, registrars and relying parties, and the availability of alternative technologies and staff resources. The article will, based on a review of standards and requirements documents, present evidence for a shortage of recovery readiness that endangers relying parties and identity ecosystems. From a review of standards and practice, we extract recovery procedures as far as they are planned for.

Keywords: digital identity; identity management; cybersecurity; disaster recovery; re-issuance; identity lifecycle

1 Introduction, problem statement and approach

Attacks against identity providers (IdP) can compromise digital ecosystems [Fr20a, Fr20b]. Relying parties lose their abilities of reliable identification and authentication of subjects until the IdP has recovered. Upon compromize, for example the European Identity Wallet has to get revoked immediately [Dr22], which in case of identity provider or technology compromize will disable a very large number of wallets, and exclude large populations from their identity ecosystems. Here, identity providers are a critical infrastructure. Identity ecosystems connect human beings to an increasing number of relying parties. High-trust domains, for example electronic government and online finance, depend on reliable digital identity. In [Fr20b], the importance of digital identities is summarized as:

> Identity management (IdM) is the key to most digital environments, the key to all citizens (military and civil), and has therefore major relevance in national security and sovereignty in the context of cyberwar.

Few examples of mass compromize of digital identities are known. One example is the temporary tax number of Norway (D-number). In 2011, 1.1 million accounts were closed

[1] Oslo Metropolitan University, Department for Information Technology, Oslo, Norway lotharfr@oslomet.no

doi:10.18420/OID2023_13

due to poor validation of identity documents presented when applying for tax numbers [MH10]. Large-scale tax fraud was committed by a league of guest workers handling multiple fake identities. The consequence was a re-identification procedure involving personal presentation of identity documents at a special police desk. In a second case, the identity provider went bankrupt as a consequence of computer intrusion. In 2012, the Dutch CA DigiNotar was found compromized [Ho12]. An attacker had gained access to all eight certification systems, and managed to create a large number of SSL server certificates. DigiNotar was taken over by the Dutch government, however quickly went bankrupt after being excluded from most application domains, specifically the SSL market. No recovery or re-issuance were performed.

Recovery efforts may require the re-registration of subjects and re-issuance of authenticators if the registration procedure or the cryptographic system have been compromised. Re-registration of millions of subjects based on paper passports or company ID cards will, however, be a demanding process. The complexities and cost of such a process will have negative impacts on the functioning, the finances and the information security of digital ecosystems in government and business.

The potential points of mass compromise are numerous. In the Taxidma threat taxonomy developed in [PH22], points of attack are summarized in 6 system levels, 6 locations, 8 identity technoology categories, and 8 attack vectors. Of particular interest are the attack categories - showing attacks against identification, authentication and governance of IdM, as well as attack vectors directed against essential components, for example the cryptographic functions used for certificate creation. The widespread proliferation of high-trust digital identity through identity brokerage spanning ecosystems and national borders has created network effects that largely increased the user base - with e.g. eIDAS having 59 eID schemes across the European Union pre-notified in January 2023[KG23]. This creates new risks. In a mass recovery situation, risk for fraudulent takeover, identity fragmentation and impersonation must be handled. Under normal conditions, such risks already demand specific attention (see [CR21]). The large-scale risk of mass recovery multiplies these risks. Consequences emerging from adversarial compromize of eID are surveillance and intelligence gathering, personalized manipulation and disruption, and mass exploitation or disruption of services[Fr20b].

The hypothesis of this article is the claim that the majority of today's digital ecosystems are ill-prepared for identity recovery through re-registration and re-issuance due to the lack of a reliable digital channel for efficient re-registration or authentication of subjects. The **research objective** of this article is: *Identify eID recovery processes and assess their feasibility for mass recovery of eID ecosystems following mass compromize of eID.*

The following text will analyze documents about identity lifec ycle models and about identification, re-identification and recovery requirements, both from standards documents, from identity providers' public documents, and from publications. Information on the procedures for identification, re-identification of persons for the purpose of eID issuance

as well as information for re-issuance and recovery procedures will be extracted from the documents. Those procedures will be discussed against the mass compromize scenario with specific focus on complexity and practical implementation prospects.

2 Findings

The main insights are: First, the absence of large-scale recovery from descriptions of identity lifecycle; there exist description of requirements for identification, re-identification and re-issuance in case of a single eID compromize, expiry or loss of authenticator. Second, Identity life cycles do not foresee mass recovery, it describes maintenance activity for active electronic identities. In search for descriptions of recovery actions, a quite diverse terminology was found. The concept of mass recovery from a large-scale compromise of identities has no well-developed language. Documentation exists for the handling of individual identity recover, re-issuance and re-identifications. Even in this case, descriptions of terms and their semantics vary from document to document. The following list of examples with definitions quoted from the referenced sources illustrates the span of terms and concepts.

Account recovery is described a procedure in [Te22b] sect. 6.1.2.3; in [CR21], section on account recovery; in [Sa21] and in [GLS19]. The descriptions cover account loss, replacement of lost authenticators, and varying levels of re-identification procedures.

Re-issuance of lost digital identities is documented at Norwegian BankID [BI22], which requires paper-based identification with customer presence, alternative ID document matching with tax authority's database for known customers, including possibility to submit verifiable documents through the on-line banking platform (p.21).

Account renewal is the term used in [Te22b] sect 6.1.4 points to 6.1.2.1. There, recommendation are given to deploy at least two authenticators for each authentication factor, for example a one-time password (OTP) device plus one of look-up-secrets, mobile device for out-of-band-authentication, or memorized secret authenticators.

Procedures focus on individual lost, expired, stolen or compromised authenticators , not large-scale recovery with central system or registration compromize. The procedures mainly point to the attribute validation in NIST SP 800-63A-4 [Te22a] in section 4.3.4.2. Admissible validation methods must be used: 1. visual and tactile inspection by trained personnel, 2. visual inspection by trained personnel for remote proofing, 3. automated document validation, 4. validation with a credible source, 5. verification of digital signatures protecting the attribute evidence. Section 4.4 lists binding rules for linking the identity with the presented evidence:

- Enrollment code verification (verifies address, phone or e-mail access within a time interval). Enrollment code not to be used as an authentication factor!

- In-person physical comparison at CSP identity proofing event.
- Remote (attended and unattended) physical facial image comparison.
- Automated biometric comparison. Biometric system comparison for in-person or remote identity proofing events.
- Demonstrate control of a digital account through the use of authentication or federation protocols, in-person or remote.

Table 1 summarizes the specific recommendations for recovery.

Procedure	**Source**	**Action**	**Stage**
Multiple authenticators per account			
Alternative authenticator (loss/theft)	NIST SP 800-63B-4 [Te22b], section 6.2	1 factor, memorized or physical, or authenticated channel	I,M
Procedures for re-issuance with and without trust			
Re-issue: trusted claim (established relation)	NIST SP 800-63B-4[Te22b], section 6.1.2.3	Re-ID based on retained information, following SP 800-63A verification step of identity proofing. For IAL3 in-person or supervised remote process: binding through video feeds, biometrics.	I,M
Suggestions for recovery tactics			
In-person verification options	[Te22b]; [HKK23]	Detailed descriptions of attribute verification	I
Account recovery provisions	[Sa21]	Multiple recovery provisions, backup authenticator, baseline customer data	I,M
Fallback channels	[HKK23]	SMS and secret phrases	I,M
Remote verification provisions	[Fo21]	Remote video, remote machine readable travel documents, biometrics, valid digital certificates, federations	I,M
eID diversity at relying party	[GLS19]	Encourage account holders at relying party to add several independent authenticators	I,M

Tab. 1: Findings for potential recovery practices, including sources. Legend; I: Issuance; M: Maintenance.

Practical issues may arise between the stakeholders, as observed by the FIDO alliance[GLS19],where the complexity of re-issuance may create serious issues on the supply chain. Low key generation rates, short supply of hardware tokens, staff shortage for in-person identification, and security issues when sending confirmation factors in a publicly known crisis scenario may arise. Other solution approaches suggest identity federations with identity brokerage as possible re-identification channels, with optional user-chosen self-sovereign identity approaches[Ku20].

3 Summary and Conclusion

The main result of this study is the insight that a mass compromise event in a critical identity ecosystem will most likely lead to major service disruptions that can last for considerable time. Businesses and government services will potentially get suspended until the identity provider has recovered, or alternative identities have been issued, accepted or activated. Recovery procedures do not scale to large dimensions, while the identity life cycle does not forsee large-scale recovery events. The practices described for general recovery were:

- The provisioning of second authenticators,
- the acceptance of emergency authenticators or external authenticators,
- the re-issuance based on trusted delivery (known address or channel),
- physical re-identification, or
- on-line remote re-identification.

Recovery strategies should include preparedness for re-issuance of identity credentials to a large subject base. To avoid personal re-registration, preparedness for digital re-enrollment must be taken. Alternative algorithms as well as a recovery platform free of compromise should be planned for. Measures should anticipate issues with physical security as well as large-scale blackouts or communication disruptions. Dependencies on the ID value chain should be assessed as a risk by relying parties.

Future research will need to distinguish life cycle phases, will have to differentiate between Identity Assurance Levels (IAL), Authenticator Assurance Levels (AAL); and Federation Assurance Levels (FAL) when producing recommendations for recovery from compromise.

Bibliography

[BI22] BITS: BankID TSPS Personal or Employee v1.6. Technical report, BITS, Oslo, Norway, 2022.

[CR21] Crow, Arynn; Rowan, John Paul: Managing Identity in Customer Service Operations. IDPro Body of Knowledge, 1(4), April 2021. Number: 4 Publisher: IDPro.

[Dr22] Drazewski, Kasper: Making European Digital Identity as safe as it is needed. Position paper BEUC-X-2022-016 - 10/02/2022, BEUC - The European Consumer Organizaton, Brussels, Belgium, October 2022.

[Fo21] Foley, Paul: REMOTE ID PROOFING. Technical report, European Union Agency for Cybersecurity (ENISA), 2021.

[Fr20a] Fritsch, Lothar: Identification collapse - contingency in Identity Management. In: Open Identity Summit 2020. volume P305, Gesellschaft für Informatik e.V., Bonn, 2020. Accepted: 2020-05-27T12:09:21Z ISSN: 1617-5468.

[Fr20b] Fritsch, Lothar: Identity Management as a target in cyberwar. In: Open Identity Summit 2020. volume P305, Gesellschaft für Informatik e.V., Bonn, 2020. Accepted: 2020-05-27T12:09:25Z ISSN: 1617-5468.

[GLS19] Gomi, Hidehito; Leddy, Bill; Saxe, Dean H: Recommended Account Recovery Practices for FIDO Relying Parties. Technical report, fido Alliance, 2019.

[HKK23] Hölbl, Marko; Kežmah, Boštjan; Kompara, Marko: eIDAS Interoperability and Cross-Border Compliance Issues. Mathematics, 11(2):430, January 2023. Number: 2 Publisher: Multidisciplinary Digital Publishing Institute.

[Ho12] Hoogstraaten, Hans: Black Tulip Report of the investigation into the DigiNotar Certificate Authority breach. Technical report, Fox IT, Delft, Netherlands, August 2012.

[IT18] ITU: Digital Identity Roadmap Guide. Technical Report ISBN 78-92-61-27831-1, International Telecommunication Union, 2018.

[KG23] Kirova, Marina; Gattwinkel, Dietmar: Overview of pre-notified and notified eID schemes under eIDAS - eID User Community -. https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS, January 2023. 2023-01-19.

[Ku20] Kubach, Michael; Schunck, Christian H.; Sellung, Rachelle; Roßnagel, Heiko: Self-sovereign and Decentralized identity as the future of identity management? In (Roßnagel, Heiko; Schunck, Christian H.; Mödersheim, Sebastian; Hühnlein, Detlef, eds): Open Identity Summit 2020. Gesellschaft für Informatik e.V., Bonn, pp. 35–47, 2020.

[MH10] Magnussen, Alf Endre; Haakaas, Einar: Fritt fram for falsk ID. In: SKUP konferanse 2010. Aftenposten, Oslo, 2010.

[PH22] Pöhn, Daniela; Hommel, Wolfgang: TaxIdMA: Towards a Taxonomy for Attacks related to Identities. In: Proceedings of the 17th International Conference on Availability, Reliability and Security. ARES '22, Association for Computing Machinery, New York, NY, USA, pp. 1–13, August 2022.

[Sa21] Saxe, Dean H.: Account Recovery (v2). IDPro Body of Knowledge, 1(8), April 2021. Number: 8 Publisher: IDPro.

[Te22a] Temoshok, David; Abruzzi, Christine; Choong, Yee-Yin; Fenton, James; Galluzzo, Ryan; LaSalle, Connie; Lefkovitz, Naomi; Regenscheid, Andrew: Digital Identity Guidelines: Enrollment and Identity Proofing. Technical Report NIST Special Publication (SP) 800-63A-4 (Draft), National Institute of Standards and Technology, December 2022.

[Te22b] Temoshok, David; Fenton, James; Choong, Yee-Yin; Lefkovitz, Naomi; Regenscheid, Andrew; Richer, Justin: Digital Identity Guidelines: Authentication and Lifecycle Management. Technical Report NIST Special Publication (SP) 800-63B-4 (Draft), National Institute of Standards and Technology, December 2022.