H. Rossnagel, C.H. Schunk, S. Mödersheim, D. Hühnlein (Hrsg.): Open Identity Summit 2020,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2020 15

Identification collapse - contingency in Identity Management

Lothar Fritsch[1]

Abstract: Identity management (IdM) facilitates identification, authentication and authorization in most digital processes that involve humans. Digital services as well as work processes, customer relationship management, telecommunications and payment systems rely on forms of IdM. IdM is a business-critical infrastructure. Organizations rely on one specific IdM technology chosen to fit a certain context. Registration, credential issuance and deployment of digital identities are then bound to the chosen technology. What happens if that technology is disrupted? This article discusses consequences and mitigation strategies for identification collapse based on case studies and literature search. The result is a surprising shortage of available documented mitigation and recovery strategies for identification collapse.

Keywords: Identity management; business continuity; cybersecurity; contingency management

```
No death, no doom, no anguish can arouse the surpassing despair
which flows from a loss of identity. – H.P. Lovecraft
```

1 Introduction

Identity management (IdM) is a critical function in many contexts. Its sudden unavailability will disrupt various processes that rely on IdM, and may cause major information security compromize or financial damage to the affected organizations or persons. I call this disruption *identification collapse*. It should be planned ahead for, and there should be resources for mitigation at hand.

This article reviews literature, standards and reports that are concerned with identification contingency. It then discusses identification collapse against case examples, both from reality as well as hypothetical ones. Specific threats and particular mitigation strategies follow the cases.

[1] Karlstad University, Dept. of Mathematics and Computer Science, Universitetsgatan 2, Karlstad, Sweden
lothar.fritsch@kau.se

1.1 Identification collapse

Definition: *Identification collapse is the unexpected disruption or loss of identity management which has negative impact on business processes and may compromize relying parties' and credential holders.*

Identification is the foundation of system access, customer relationships, supplier inclusion, payments, and increasingly the basis for the management of devices on the Internet of Things. Identification collapse will disrupt those processes, and therefore needs attention.

1.2 Background: Literature overview

In this section, a background search for identification failure, contingency and mitigation strategies is presented. There is a surprisingly low number of publications that investigate preventative, corrective or compensatory strategies for identification failure available in scientific literature. Security standards demand unspecific safeguards to be taken. A literature search on e-ID contingency has been performed on Google Scholar using the search keywords below:

digital identity contingency, digital identity management contingency, digital identity management business continuity, digital identity management disaster recovery, identity provider compromised business continuity, identity provider compromise disaster recovery, identity correlation, digital identity substitution, digital identity replacement, Identity Relationship Management

The search resulted in zero scientific publications from the computer science, technology or information systems domain that were clearly focused on the collapse of IdM and of its contingency management. In the patents category, a number of patents that deal with recovery passwords and additional authentication factors for credit cards appeared. The search was then repeated on the regular Google.com search engine with the same list of keywords. This resulted in a large number of reports from consulting firms that offer business continuity services for various core IT services. IdM systems were briefly and in very unspecific ways mentioned as critical assets in the context of the IT managment standard ITIL for business continuity management. The most advanced perspective on identification contingency was found in documents from the financial sector, namely in reports from the EU project *Parsifal* (2008-2010, by now expired from the Internet), and in later proposals for governments that offer the financial sector's IdM services to governments and to global actors [Mc16]. Searching for particular actions that support recovery from a total breakdown of IdM that will require re-issuance of credentials, notable only the United Nation's UNHCR disaster relief agency has a clearly formulated strategy for the mass issuance of new digital identity under adverse conditions [UN18]. An estimate of the efforts of re-issuance can be gained from section 2, 'Registration and Issuance Requirements' in the Federal Identitiy Management Handbook [FICCB05]. The Australian Identity Proofing

Requirements require identity providers to document their recovery and disaster procedures in an operations handbook [Au18]. The operations manuals are not published, though. They recommend:

Establish and maintain an Identity Service Provider Operations Manual, which at a minimum includes the following information: (...) Processes, procedures and workflows used to support the IdP's identity management functions (i.e. access control, storage, backup, archive and retrieval, disaster recovery, business continuity and records management) (...)

The International Civil Aviation Organization defines guidelines for thorough identification of flight passengers [IC18], which provide further insight into re-registration efforts. No dedicated mention of strategies or technologies for redundant IdM infrastructures, suppliers or fallback mechanisms with proportional security levels were found in the search. Summarizing the search I conclude that there is very little explicit guidance on disaster preparedness, recovery, mitigation and business continuity published that specifically targets identity management as a critical infrastructure.

2 Case examples of Identification collapse

This section will illustrate the concept of identification collapse. For this purpose, three case studies about collapses relevant to the end user are used to describe identification collapse. The following autoethographic case studies [Ma10] show identification collapse and discuss its consequences specific to the use case. Autoethonography is, according to [Ma10], *a form or method of research that involves self-observation and reflexive investigation in the context of ethnographic field work or writing*. It refers, among others, to *reflexive accounting of the narrator's subjective experience and subjectivity. (...) Systematic, self-conscious introspection enables the disciplined analysis of personal resonance and the effects of the researchers' connections wit the research situation on their actions and interpretations, in dialogue with the representations of others*.

2.1 Case 1: Swedish Railway - customer profile passwords insecure

A Swedish railway company servicing international connections offers customer web pages with individual ticketing services, payment options and loyalty program functions. Customers can pay loyalty points to obtain tickets, review their travel history or order and download tickets. Authentication is based on e-mail/password, while payments are authorized via credit cards' mechanisms. Customers provide a citizen number and address when registering for the loyalty program. In 2019, the railway carrier detected password hacking activities with the goal to issue tickets with loyalty points from hacked customer web accounts. As a reaction, spending loyalty points was restricted to the mobile phone app, and required a Swedish BankID installed and activated on the phone. The BankID is only

available to persons who are living in Sweden, have a Swedish citizen number issued, and who use a Swedish mobile phone subscription. Other customers are referred to the telephone hotline for assisted ticketing. By moving from a cheap one-factor password solution to a national identity silo that has strong dependencies (citizen number, bank account, local phone card), the railway company alienated most of its international customers. In addition, they increased costly traffic on their phone hotline, where callers identify by speaking their loyalty number and a PIN code, which both are visible in the customer profiles once an attacker has logged in. The situation persists as of January 2020. So far, no alternative authentication methods or other efforts have been communicated that may ease the situation. The company has no alternative identification strategy.

Summary: Train company has no digital back-up identification channel. All international customers, such as cross-border commuters, are excluded from on-line booking and app booking services based on the loyalty program. Cost occurs for phone service. Alternative identification via phone is equally insecure as web passwords. Duration of problem: very long. Tab. 1 shows an assessment of the compromized IdM services.

Cause (internal, external)	Scope		Affected IdM phase				
	Small scope	Global scope	Registration	Issuance	Provision	Termination	Archive
I: Weak authentication compromized, fallback to telephone service		X	Attributes may be changed by attacker	Credential available to others	Identification compromized	-	Archive accessible to other parties, archive content potentially compromized.
Consequences	Large-scale identification collapse for foreign customers. Business process endangered, identity compromized in four out of 5 phases, alternative oral password authentication via phone, foreign and 'dumb phone' customers alienated.						

Tab. 1: Classification of Swedish railway identification failure.

2.2 Case 2: Norwegian BankID - token battery low

The Norwegian BankID uses a code generator as a second, personalized and hardware-based authentication factor. It is issued based on a bank account, which in turn is based on citizen numbers or passport identification. BankID offers authentications to other sectors, including government. It is the most commonly used electronic identity for signing up to new services in Norway. However once the token battery is low, the renewal of the token is performed in a disruptive way: The existing token is deactivated immediately when ordering a new

token - which then is sent by physical mail with expected three days delivery time, including the usual risks of lost mail, postal strike, weather-caused and seasonal delivery delays. For the delivery period, the BankID owner technically is unidentifiable for banks, private sector or government services. The bank offered a back-up identification channel: it advised its customer to use a Mobile BankID in the meantime, an alternative credential that is issued based on BankID to Norwegian phone subscribers with smart phones. However, the customer was not advised to install and activate Mobile BankId before the BankID token was blocked. Neither had the bank a suggestion for users who may use other phones or foreign phone cards.

Summary: Bank has an equally secure back-up credential based on BankID, which however has dependencies towards phone subscriptions and phone hardware which impose customer cost. The risk of being unidentifiable is limited to a few working days while the postal distribution works as expected. Tab. 2 shows an assessment of the compromized IdM services.

Cause (internal, external)	Scope		Affected IdM phase				
	Small scope	Global scope	Registration	Issuance	Provision	Termination	Archive
I: Token renewal procedure causes delay or imposes cost	X		-	Issuance has delay OR demands expensive alternative channel	Identification prevented	-	-
Consequences	Short period of service denial for users without national smartphone solution.						

Tab. 2: Classification of bank token replacement identification failure.

2.3 Case 3: Norwegian BankID registration issue - re-newal of registration

One immigrant customer of a Norwegian bank had opened additional bank services within his bank with his BankID token. After Norway changed regulations for identity verification, banks had to re-assess customer identity. This process led to the discovery of the fact that the aforementioned customer's citizen number was incorrect in the BankId certificates due to issuance of a new citizen number. However the bank's procedures did not allow for change of citizen numbers bound to accounts and financial assets. Different departments were handling the update of the identity attribute 'citizen number' in different ways. Regular accounts were deleted and set up anew (with significant delays until old correspondence had been manually retrieved from back-up). Investment assets were preserved, while the

investment department had procedures for re-registration that demanded physical presence and passport-showing for the re-issuance of the authorization to access the financial assets.

Summary: Bank had no procedures for change of core identity attributes (or, in a wider perspective, for a registration failure with credential issuer). Various procedures for recovery applied which involved several days of inconsistent access to services and documents as sell as required a physical visit to the bank to verify passports. Tab. 3 shows an assessment of the compromized IdM services.

Cause (internal, external)	Scope		Affected IdM phase				
	Small scope	Global scope	Registration	Issuance	Provision	Termination	Archive
I: Identity attribute expired	X		Registration compromized	Identification revoked	Provisioning denied	-	-
Consequences	Several day of identification collapse leading to major manual procedures for content recovery, identity mapping and re-resgistration of customer.						

Tab. 3: Classification of banking attribute renewal identification failure.

There has been, in addition, a major collapse with an issuer of commercial web certificates, *DigiNotar*, which was hacked and then used to issue large numbers of fake certificates. Only after several months this was discovered, and business terminated by the Dutch government[2]. Here, registration and issuance were compromized, then provision stopped. Certificates were not person certificates, though.

3 Causes and Consequences of identification collapse

Consequences of identification collapse have a wide bandwidth of impact on business continuity. As seen from the cases above, impact ranges from shorter waiting times for renewal to multi-month identification failure.

3.1 Types and magnitude of identification collapse

Generalizing the root causes, identification collapse can be caused by the following causes of failure:

Technological failure: Breakdown of core technologies involved in IdM, including compromized cryptography;

[2] See full descripition: https://www.enisa.europa.eu/media/news-items/operation-black-tulip, accessed 03-Apr-2020

Procurement failure: Externally procured IdM is unavailable or compromized. IdM is procured along a supply chain from external providers, either as the whole service, as a cloud service or in part through technological platforms or processes controlled by suppliers;

Administrative failure: Wrongly executed procedures under registration, revocation or attribute handling compromize digital identities and relying services.

Force majeure: Operations of IdM are discontinued due to higher forces such as natural disasters, war, bankruptcy or global crisis.

The magnitude of the collapse can appear in a wide range. As illustrated in the case examples above, only parts of the user base may become excluded. Technological issues or registration problems may appear locally only. On the other hand, compromized cryptography, lack of back-up authentication methods, comprimized registration data of the whole user population or technological disasters may shut complete services down, which creates a negative event of high magnitude. Magnitude is best expressed in the number of digital identities affected as well as in how much of an identity ecosystem will be affected for how long:

magnitude =
(number of users affected $\bigotimes$ number of services affected $\bigotimes$ duration of collapse)

Risk managers should therefore model the magnitude of identity collapse not only from a perspective of data compromize, privacy breach or access control failure, but in addition in the perspective of loss of service and exclusion of customers in face of the planned recovery channels for identification. Commonly appearing consequences of major identification collapse will be: Access control systems compromized; External relationships break (customer relations); Critical services stop (payment, public services, private services, signing); Historic authorization and non-repudiation endangered (prior signatures or transactions or certificate validity back in time not verifiable) (see 7.3.5 in [Wi07]).

4 Mitigation and business continuity

Due to the very small body of literature found in the literature search (see Sec. 1.2, this section will present reasoning and options for handling identification failure for the sake of business continuity. While there are many operational requirements such as ensuring equivalence in information security parameters such as trustworthiness, security, usability and privacy, in addition aspects of integration, cost, time-to-deployment, of international availability and regulatory issues will come into play. The analysis in this section focuses on the phases of identity management in a perspective of technical and administrative controls to prevent, mitigate or compensate identity collapse. When looking for mitigation of identification collapse, certain requirements occur naturally:

- equivalence of security, privacy, usability and integration/application cost;
- short time-to-availability in case of replacement;
- availability to user base, e.g. hardware tokens, cross-border availability for customers or users from other countries.

In addition, a crisis communication strategy [WP17] that targets the user base and the relying parties has to get planned. Depending on the root causes, other communications such as data breach notifications must be included [Fu16, KJP17].

4.1 Technologies for mitigation

Technological solutions or identity contingency are available. Below a variety of building blocks will be summarized. They include identity federations [Su05], identity brokerage, biometric anchoring, identity correlation and blockchain-based approaches.

Identity brokerage: The FutureID research project has developed an identity brokerage infrastructure that uses a centralized Identity Broker that has the ability to extract identity attributes from various identity providers [BR16]. Thereby it is able to extract attributes from the same person's various digital identities, connecting them into a new synthetic identity. The Identity broker could be used such that upon technical compromize of an IdM system it would request identifications from other identity silos based on the just compromized identity. This method requires a pre-established brokerage federation, though. It does not overcome issues with archive compromize, and does not help in situations where identity registation is compromized. It is however an effective way to establish a short-term emergency identification mechanism.

Biometric authentication factors: Using biometric authentication as an additional authentication factor for re-registration will help re-establishing credentials. While biometrics are not without issues (reliability, survellance and privacy issues), they could be used as a recovery channel for more efficient registration or issuance.

Verifiable cryptographic identity correlation: Identity correlation connects identities across silos, and thereby supports swift contingency management[3]. Keybase [4] is a service that allows its users to cryptographically verifiably prove ownership and correlation of digital identities such as social media accounts. Credential owners can create links between their existing identities. However, replying parties must prepare to accept Keybase proofs, and then be ready to connect to the alternative identity silos. Identity correlation is therefore weaker as brokerage as it only shows correlation, but does not provide federation services.

[3] Identity correlation, `https://en.wikipedia.org/wiki/Identity_correlation`, 20200131
[4] See `https://github.com/keybase/client`, 20200131

Block chain securiztation of IdM: Archival of relevant status information can be facilitated with block chain technology [EHEK19, NJ19]. Several approaches are under scientific investigation:

- Cross-referencing identities as equivalent through a public block chain by credential issuers (thereby creating the foundation for federations);
- Recording of identity history in a block chain for rollback;
- Self-sovereign identity management (SSI) enables credential holders to register and publish their credentials on block chains for reference for others [NJ19].

Mapping digital identities into each other and at the same time keep track of relevant trust information in block chains may solve a number of issues when recovering from registration or archive compromize. As discussed in [Fr13], growing complexity of the identity ecosystem will degrade the quality and value of identity management. SSI may enable credential holders to reference an alternative IdM silo and would in consequence enable the acceptance of an alternative credential by the relying party.

Standards for identity federation and brokerage: Standardized formats, protocols and algorithms for IdM will help prevent identification collapse. Compatible infrastructures as suggested in OPAL [HP18] will enable swift recovery from infrastructure or technology failure.

4.2 Administrative measures

In addition to technological preparedness, administrative measures that lower risk of identity collapse as well as procedures for mitigation and recovery must be in place. For each phase of the IdM lifecycle, thorough analysis of the administrative issues with identity collapse should get performed, in particular:

- Planning for ID continuity with back-up channels and back-up registration methods with high throughput and appropriate geographical spread;
- Deployment of identity brokers that help include the best possible alternative across multiple industrial digital identities (e.g. inclusion of banks, mobile operators, government IdM);
- Consideration of eIDAS as a recovery channel for persons who own multiple, independent government credentials (however eIDAS is mostly designed to project national sovereign IdM into other countries);
- Train staff for migration activities, such as re-registration of users based on identity documents or a variety of electronic identities.

Further considerations that are important are alternative authentication channels used for either using back-up channels, to federate or broker identities, or to re-register efficiently.

Availability of alternative identification channels: Review of existing back-up channels (alternative or multiple IDs) for customers will support the establishment of recovery channels (e-mail, multiple e-mail, phone numbers for SMS, security phrases, "recognize your friends"). What will be the 'anchor' identity (e.g. passports, bank IDs, social security numbers)?

Emergency registration procedures: The UNHCR has very explicit procedures for the set-up and registration of large populations of refugees in cases of disaster. Biometrics are used to anchor registration into IdM systems [Lo16] as part of the United Nation's UNHCR Guidance on Registration and Identity Management [UN18]. In its Future of Financial Services Series, the World Economic Forum (WEF) has analyzed the potential and the roles of the global and national financial institutions in identity management [Mc16]. In its report, the WEF concludes that the most resilient, reliable and user-friendly structure of IdM should either be organized as a silo or as a network of collaborating providers using standardized technologies (pp. 62, centralized or distributed identity).

4.2.1 Problems caused by mitigation

Mitigation strategies may have side effects. They open up identity silos, and may therefore cause issues concerning information privacy, secrecy or even sovereignity over IdM ecosystems. Landau and More [LM12] identify several issues that impair economic success of federated IdM: Issues of trust and liability across federations occur as well as reliability and the distribution of duties/benefits between participants. Data privacy when sharing attributes in federations is a major issue.

- Identity silo collapse: Federation or correlation of separate identities for contingency may lead to identity leakage, pseudonym compromize or privacy breaches (see [Ja15] for example on how swift biometrics deployment in a no-alternative-choice disaster relief registration campaign takes decision power from individuals).
- Degradation of security level through contingency solution;
- Exclusion and discrimination of parts of the user base through chosen alternative channels, e.g. through geographic limitations, nationality or individual disability [FFS10].

In addition, fraud protection will face major challenges in case of mitigation through alternative identification channels. The only viable solution in this context will be the pre-establishment of trust in IdM quality through common standards and procedures, e.g. in

industry sector organizations such as the financial industry, in the government sector and in critical infrastructure protection.

5 Conclusion

Identification collapse is a serious threat to business continuity. It can be caused by technical and non-technical issues. This article shows that there is little scientific work on preventive and contingency strategies and options to prevent or to mitigate identification collapse,in spite of available technologies and tactics. Cases have shown that relying parties show a wide spread in their preparedness for alternative identification channels or for business continuity. A general impression persists that either weak and cheap identification methods are used (social media single-sign-on, passwords or phone numbers), more secure two-factor authentication being restricted to national silos in spite of European Union efforts, and finally the back-up channel being off-loaded to smartphones paid for by the credential holder. In various industry standards, general precautions and measures are suggested, however not specified. Most concrete are guidelines for identity verification documents upon registration from a variety of organizations, including air travel and international disaster relief. In summary, there is a lack of knowledge in various important aspects of Identification collapse that should be further investigated. Strategies, technology and processes for emergency re-registration or federation of identities will be important, as well as strategies, technologies and solutions for redundant identification, such as digital identity correlation, federation and brokerage between identity silos, industry sectors and governments. Trust status aggregation and risk information about the identity ecosystem supply chain nodes will complement contingency measures.

Identity Management continuity should be regarded as a priority in national cybersecurity policy, and in particular where involved in the operations of critical infrastructures, as identification failure with long recovery times will have catastrophic consequences for most digital infrastructures.

References

[Au18] Australia: Identity Proofing Requirements - Trusted Digital Identity Framework v1.07. Technical report, Digital transformation agency, 2018.

[BR16] Bruegger, Bud P.; Rossnagel, Heiko: Towards a decentralized identity management ecosystem for Europe and beyond. Gesellschaft für Informatik e.V., Bonn, pp. 55–66, 2016.

[EHEK19] El Haddouti, Samia; El Kettani, M Dafir Ech-Cherif: Analysis of Identity Management Systems Using Blockchain Technology. In: 2019 International Conference on Advanced Communication Technologies and Networking (CommNet). IEEE, pp. 1–7, 2019.

[FFS10] Fritsch, Lothar; Fuglerud, Kristin Skeide; Solheim, Ivar: Towards inclusive identity management. Identity in the Information Society, 3(3):515–538, 2010.

[FICCB05] Federal Identity Credentialing Committee, Office of Management; Budget, U.S. Government: Federal Identity Management Handbook (public draft). Technical report, Federal Identity Credentialing Committee, Office of Management and Budget, U.S. Government, 2005.

[Fr13] Fritsch, Lothar: The clean Privacy Ecosystem of the future internet. Future Internet, 5(1):34–45, 2013.

[Fu16] Fuller, Ryan P: The big breach: An experiential learning exercise in mindful crisis communication. Communication Teacher, 30(1):27–32, 2016.

[HP18] Hardjono, Thomas; Pentland, Alex: Open algorithms for identity federation. In: Future of Information and Communication Conference. Springer, pp. 24–42, 2018.

[IC18] ICAO: ICAO TRIP Guide on EVIDENCE OF IDENTITY v5.3. Technical report, ICAO Security and Facilitation, 2018.

[Ja15] Jacobsen, Katja Lindskov: Experimentation in humanitarian locations: UNHCR and biometric registration of Afghan refugees. Security Dialogue, 46(2):144–164, 2015.

[KJP17] Kim, Bokyung; Johnson, Kristine; Park, Sun-Young: Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity. Cogent Business & Management, 4(1):1354525, 2017.

[LM12] Landau, Susan; Moore, Tyler: Economic tussles in federated identity management. First Monday, 17(10), 2012.

[Lo16] Lodinová, Anna: Application of biometrics as a means of refugee registration: focusing on UNHCR's strategy. Development, Environment and Foresight, 2(2):91–100, 2016.

[Ma10] Marechal, G: , Autoethnography. Albert J. Mills, Gabrielle Durepos and Elden Wiebe (Eds.), Encyclopedia of case study research (Vol. 2, pp. 43-45), 2010.

[Mc16] McWaters, Jesse: A Blueprint for Digital Identity - The Role of Financial Institutions in Building Digital Identity. Technical report, World Economic Forum, 2016.

[NJ19] Nauta, Jelle C; Joosten, Rieks: Self-Sovereign Identity: A Comparison of IRMA and Sovrin. Technical Report TNO2019R11011, 2019.

[Su05] Sullivan, Roger K: The case for federated identity. Network Security, 2005(9):15–19, 2005.

[UN18] UNHCR, United Nations: UNHCR Guidance on Registration and Identity Management. Technical report, United Nations UNHCR, 2018.

[Wi07] Wisse, Pieter: Semiotics of identity management. In: The History of Information Security, pp. 167–196. Elsevier, 2007.

[WP17] Wang, Ping; Park, Sun-A: Communication in Cybersecurity: A public communication model for business data breach incident handling. Issues in Information Systems, 18(2), 2017.