Vidan G. Identity as a Service: Iceland's Kennitala and the Convergence of Identifier and Authenticator in Online Third Party Applications. *Technology Science*. 2015092902. September 29, 2015. http://techscience.org/a/2015092902

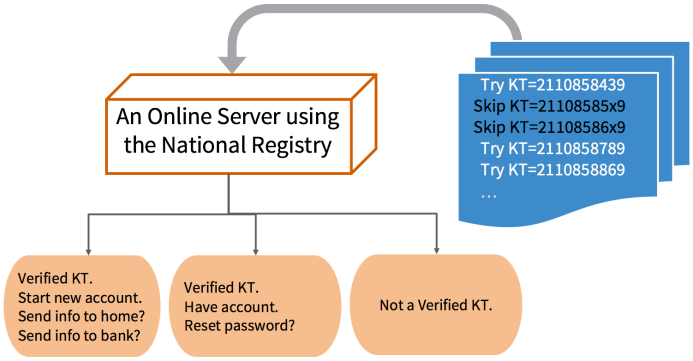
Identity as a Service: Iceland's Kennitala and the Convergence of Identifier and Authenticator in Online Third Party Applications

Auðkenning sem þjónusta: Kennitalan á Íslandi – munurinn á auðkenni og staðfestum uppruna við notkun hugbúnaðar þriðja aðila á netinu

Gili Vidan

Highlights

- Iceland's national identifier, the Kennitala (KT), is computed from one's date of birth and some random digits
- I found five Icelandic subjects online and was able to guess and verify their KT using a dating app
- This experiment suggests that KT registry may be reverse-engineered and expose personal data on services that rely on the KT for authentication to imposters



Using an online server to identify which potentially valid national identifiers are assigned.

Abstract

Iceland has a national identifier, called the Kennitala (KT), which assigns a unique number to each resident. The government provides an online service to verify whether a KT, date of birth, and name are in the national registry. In daily use, the KT often appears alongside a name to identify a person. People and businesses in Iceland may also obtain a copy of the entire registry of names and KTs. Unlike many other countries that have national identifiers, Iceland does not consider KTs to be private information. Therefore, having copies of registries and an online service to verify registry entries may not seem problematic. However, doing so changes the role of the KT. Identifying an individual from among many possible people is a task well suited for a name or KT. But the public nature of the national registry makes it harder to verify that an arbitrary online user is exactly the person who is assigned that name and KT. For example, a dating app based on the Íslendingabók genealogy website traces Icelandic genealogical relations based on users' KTs. The app, intended for use only by registered residents of Iceland, requires a KT. Auroracoin, a cryptocurrency intended for Icelanders to use to make financial purchases, authenticates users by matching the user's KT with her name as provided by a Facebook profile. What happens when an arbitrary online user correctly infers an individual's KT and attempts to gain access to these services?

Results summary: A KT number is 10 digits. The first six digits are the date of birth (DOB), the next two digits are random values, the next digit is a checksum (an arithmetic operation using the DOB and the random digits), and the last digit specifies the millennium of birth. I searched for Icelandic names online and found five subjects. For each subject, I had at least the person's name and date of birth. I computed possible KTs for the individual and then attempted to register on Íslendingabók with the information. If the person already had an account, the system revealed the person's first name and provided an option for me to reset the password. If the person did not have an account, I was offered the option of having information sent to the home address on file at the registry or to the bank account on file at the registry. This small experiment suggests that someone outside Iceland could reverse-engineer large parts of the registry without directly interfacing with governmental services. When third-party services rely on the KT for authenticating users, they can leak personal information to impostors.

Abstract (Icelandic)

Á Íslandi er fólk auðkennt á þjóðarvísu með svokallaðri kennitölu, sem úthlutar einstöku númeri til hvers íbúa. Stjórnvöld bjóða upp á þjónustu á netinu þar sem hægt er að ganga úr skugga um hvort kennitala, fæðingardagur og nafn séu í þjóðskránni. Í notkun dags daglega er kennitalan oft sett við hliðina á nafni til þess að auðkenna einstakling. Einstaklingar og fyrirtæki á Íslandi geta einnig fengið skrána yfir öll nöfn og kennitölur í heild sinni. Ólíkt mörgum öðrum löndum sem nota auðkenningu á þjóðarvísu teljast kennitölur ekki vera leynilegar upplýsingar. Því virðist það ekki vera vafasamt að eiga afrit af skráningum og að rafræn þjónusta sé til staðar til að sannreyna kennitölur. Þar sem þetta er samt sem áður reyndin breytist hlutverk kennitölu. Það að bera kennsl á einstakling meðal margra

mögulegra einstaklinga er verkefni sem hæfir vel nafni eða kennitölu. En það að þjóðskráin er opinber gerir erfiðara um vik að sannreyna hvort handahófskenndur notandi á netinu sé nákvæmlega sú manneskja sem fékk úthlutað nafninu og kennitölunni. Til dæmis er til stefnumótasmáforrit („app"), sem byggir á Íslendingabók og rekur ættartengsl fólks byggt á kennitölu notanda. Smáforritið, sem eingöngu er ætlað skráðum íbúum á Íslandi, krefst kennitölu. Myntin Áróra, dulkóðunargjaldmiðill sem ætlaður er Íslendingum til fjármálakaupa, staðfestir uppruna notenda með því að para kennitölu þeirra við Facebook ágrip þeirra. Hvað gerist þegar handahófskenndur notandi á netinu gefur upp rétta kennitölu einstaklings og reynir að fá aðgang að þessari þjónustu?

Ágrip af niðurstöðum: Kennitala er 10 tölustafir. Fyrstu sex tölustafirnir eru fæðingardagur og fæðingarár, næstu tveir tölustafir eru valdir af handahófi, næsti tölustafur þar á eftir er prófsumma (reikniformúla sem reiknuð er út frá fæðingardegi, fæðingarári og tölunum sem valdar voru af handahófi) og síðasti tölustafurinn tilgreinir öldina við fæðingu. Ég leitaði að íslenskum nöfnum á netinu og fann fimm íbúa. Fyrir hvern og einn var ég að minnsta kosti með nafn viðkomandi og fæðingardag. Ég reiknaði út mögulegar kennitölur fyrir einstaklinginn og reyndi síðan að skrá mig inn í Íslendingabók með upplýsingunum. Ef viðkomandi var nú þegar með aðgang birti kerfið fornafn hans og bauð upp á að ég gæti sett nýtt aðgangsorð. Ef einstaklingurinn var ekki með aðgang var mér boðið upp á að fá upplýsingarnar sendar á heimilisfangið sem er í skránni eða á bankareikninginn sem er í skránni. Þessi litla tilraun bendir til þess að aðili utan landsteinanna gæti gert stórar breytingar á skránni án þess að hafa beint samband við opinbera þjónustu. Þegar þjónusta þriðja aðila reiðir sig á kennitölu til að staðfesta uppruna notenda, getur hann lekið persónuupplýsingum til svikara.

Introduction

Like many countries, Iceland assigns unique national identifiers to individuals and businesses. However, unlike most other countries', Iceland's numbers are not a secret [1]. Its system is called the Kennitala (KT); the name is a combination of the Icelandic words for "identity" and "number." The national registry that contains the names and KTs of all registered residents in Iceland can be accessed by Icelandic citizens through a relatively simple application. There is no attempt to mask the number. There is no stringent regulation about disclosing names or inferring KTs. Even though a KT is personal information pertaining to an individual, it is not considered sensitive information.

In comparison, the United States issues Social Security numbers (SSNs) that individuals and businesses often hold in secret. Americans do not usually disclose SSNs publicly because the confidentiality of financial, tax, and other records relies on the concept that the SSN is private information the person knows. This assumption is what allows such services to use the SSN as an authenticator, that is to say, knowledge of the SSN is the means through which one's identity is established. This use as an authenticator increases the risk of harm to the

individual if the SSN becomes known. There have been widespread data breaches of information containing SSNs, putting many Americans at risk of identity theft and threatening the efficiency of the services that rely on them [3][4][5][6].

KTs do not have a secrecy requirement because by design they are intended to be used only as a unique identifier (similar to knowledge of one's name, except that they are guaranteed to be unique). The rise of online services requiring a means of verifying the real identity of users has created a situation in which the KT's function is stretched beyond its original purpose. In combination with other personal information, it functions as both an identifier and an authenticator. Can impersonators compromise such systems that employ KTs beyond their original identifying function? Consider two Icelandic online services that include the KT as part of their requirements for registration.

Íslendingabók is an online genealogical website, started in 1997 by a private programmer and now owned by the biopharmaceutical company deCODE Genetics. The website includes lineage information on the majority of the Icelandic population [7]. One use of the database is by a dating app that displays degrees of kinship between the user and others [8][9]. The app allows users to obtain information by bumping their devices or conducting a name search. All registered Icelandic residents may use the app. The user provides her KT and other information. A centralized government system then offers two ways for her to be authenticated as the person approved for use with the KT. She may either receive a message through her Icelandic bank account associated with the KT or she may receive physical mail with a code at the home address associated with her KT.

Auroracoin is a cryptocurrency launched in 2014 and designed to provide a decentralized alternative to the heavily regulated monetary system that Icelanders have been subjected to since the 2008 Global Financial Crisis [10]. To begin the currency's circulation, its developer designed a system for distributing a portion of the currency to each Icelandic registered resident. The developer used the KT registry to get the numbers associated with Icelanders, but the developer could not rely on bank accounts for authentication. Therefore, Auroracoin turned to Facebook Connect, a popular social network system based on profiles that people make themselves with an email address. Such a design rests on the assumption that any user of Auroracoin will have a Facebook account that uses her real name as it appears in the KT registry. Thus, Facebook acts as a third-party identity authenticating service that confirms for Auroracoin that the log-in information the user has entered to Facebook Connect correlates with an account under a given name. Auroracoin then checks the provided KT and the name provided by Facebook's service against the registry.

These two online services use the KT in different ways to determine whether a user is the person associated with the KT. Íslendingabók uses a government-backed service that relates KTs to bank accounts and residential addresses. Auroracoin uses KT numbers and Facebook profiles. Can an impostor be registered on either of these systems?

Background

The way in which Iceland issues a KT number is well known, and changes to the system have been documented in scholarly work [1]. The KT number has 10 digits. The first six are the person's date of birth (DOB) in the format DDMMYY, where DD is the 2-digit day, MM is the 2-digit month, and YY are the last two digits of the year. After the DOB are two randomly generated "birth number" digits with a limited range that distinguish those sharing the same DOB, a check digit (an arithmetic operation using the DOB and the two "birth number" digits), and lastly a millennium number (e.g. 9 for those born before the year 2000).

If abcdefgh are the first 8 digits of a KT, then the checksum digit is $11- ((3 \times a + 2 \times b + 7 \times c + 6 \times d + 5 \times e + 4 \times f + 3 \times g + 2 \times h) \% 11)$ where % is the remainder or modulus operator. The two "birth number" digits have a limited range: the first goes from 2-9 and the second from 0-9. A remainder of 0 would set the checksum digit at 0, and a remainder of 1 would lead to a two-digit checksum of 10, which would be deemed invalid. A new birth number would be chosen and the calculation would be done again [2]. With these restrictions in place, the number of possible assignments drops from 100 to 72. This means a typical birthdate has about 72 possible KTs.

As an example, consider the KT 2110858439. The person's date of birth is October 21, 1985, and the two random digits are 8 and 4. I can confirm whether this could be a valid KT using the checksum calculation. The checksum digit is 3. The calculation is:

$11- ((3 \times 2 + 2 \times 1 + 7 \times 1 + 6 \times 0 + 5 \times 8 + 4 \times 5 + 3 \times 8 + 2 \times 4) \% 11)$

$= 11- ((6 + 2 + 7 + 0 + 40 + 20 + 24 + 8) \% 11)$

$= 11- (107 \% 11)$

$= 11 - 8$

$= 3$

Therefore, 2110858439 is a possible KT. For the given DOB there are 73 possible KTs that would satisfy the checksum requirement.

Methods

Both Íslendingabók and Auroracoin require a person to register using a KT. Not being from Iceland, and residing in a different country thousands of miles away, can I impersonate someone on Íslendingabók using only inferred or publicly available information?

My approach has three steps:

1. Search online to find known instances of name, KT, and date of birth
2. Produce a list of potential valid KTs for a given date of birth
3. Use Íslendingabók to verify KTs.

Step 1: Search online to find known instances of name, KT, and date of birth

Because KTs are not private information, I expected to find instances of them online with the person's name and, depending on the content, the person's date of birth.

Step 2: Produce a list of potential valid KTs for a given DOB

I wrote a script based on the encoding description of KTs described earlier. For any given DOB, there are 100 possibilities for the random digits, however, not all these 100 possibilities will satisfy the checksum digit requirement. Testing my script on 5 birth dates, my script produced between 70 and 79 possible KTs that adhere to the checksum requirement for a given DOB.

Of course, just because a KT adheres to the checksum equation does not mean the number is actually used. Iceland has a small population of about 330,000 residents with a KT. If we have the system account for 100 different years, my script will generate about 365 days times 100 years times 79 valid KT configurations or 2,883,500 valid KTs. Few of those will actually match real people in Iceland. Therefore, rather than trying all valid KTs, I will locate actual DOBs of known Icelandic people to narrow the possibilities when testing the online service's likelihood to verify my artificial emulation of the KT.

Step 3: Use Íslendingabók to verify KTs.

The Íslendingabók uses a government back service to identify invalid registration attempts. Because of this service's online design, I can use it to test which of my generated KTs map to real people having those KTs. The system provides me a way to verify a usable KT without interfacing directly with the national registry.

The possible Íslendingabók responses to my registration attempts are: (1) the KT number is invalid, which means it does not exist in the national registry; (2) the KT number is valid and open for registration, which means the number is assigned to a person who has not registered for the service; or (3) the KT is valid and already used by a registered user of the service, which when used also reveals the user's first name.

Results

On September 24, 2015, I used Google to search for common Icelandic names [11][12]. These included first names such as "Sigrún" and "Jón." "Stefánsdóttir" and "Jónsson" were typical

last names, which in Iceland are composed of a parent's first name and a familial suffix. I conducted seven searches and visually inspected 15 results until I found five individuals whose full names and KTs were available. These comprise the five subjects of my study. Having found information for these five subjects as a benchmark, I then tested my script, generating all possible KTs for the given DOB of each of the five subjects.

Because this paper demonstrates the problematic nature of this information, in reporting results in this paper I will refer to the subjects merely as Subject1, Subject2, Subject3, Subject4, and Subject5. (For privacy reasons, identifying details for the five subjects are not printed here but are available to qualified reviewers to verify my results; see the link in the data section of this paper.)

I tested my KT generator script on the birthdays of the five subjects. My script produced 73 potential KTs for Subject1's DOB, 73 potential KTs for Subject2's DOB, 72 for Subject3, 72 for Subject4, and 73 for Subject5.

Attempting to register new accounts with Íslendingabók for each of the subjects involved trying each of the KTs for each subject.

The system ignored all KTs for which there was no matching information in the national registry. In each case, it ignored all other potential KTs for the subjects except the single KT for each subject reported in the data section. In this way, Íslendingabók acted as a verifier of KTs, allowing me, without having to refer to my benchmark data, to distill my list of potential KTs to the one existing number.

The system responded to one of the KTs for Subject2 by indicating that Subject2 was eligible to move forward with a new account. It then asked whether I wanted the registration information mailed to the home address on file at the national registry or delivered electronically to an Icelandic bank account associated with the KT. In such a way no new personal information was revealed to me, except the fact that the number existed and that Subject2 had not previously registered for the service.

The system responded to one KT each for Subject1, Subject3, Subject4, and Subject5 by indicating they were already registered users. It then displayed a message that provided the first name of the person associated with the KT and asked whether I wanted to reset the password for the account. While I did not attempt to reset these passwords, as they corresponded to real users' accounts, this result did further confirm the relation between my subjects' artificially generated KTs and their registered names.

Discussion

My experiment revealed privacy vulnerabilities with Íslendingabók. Publicly available information that contained the name and dates of births of Icelandic residents was used to

generate possible national identifiers for them (KTs). An online central service allowed me to indiscriminately make inquiries to learn the combinations of name, KT, and date of birth that corresponded to known people.

If KTs were considered private information, more like the SSN in the US, would this vulnerability be possible? My experiment shows that deeming the KT to be private information would not have thwarted the experiment because I made guesses at the KTs and was able to construct them.

Of course, the design combining date of birth and the checksum requirement reduced the number of possible KTs I had to test. However, what allowed me to know whether a guess at a KT was correct was access to the centralized service. It allowed me an unlimited number of guesses. A simple remedy for this vulnerability would seem to be to limit the number of inquiries that can be repeatedly made. A first step is to limit requests from the same machine's IP address. Further work is necessary to prevent the same attack being done from many different machines.

In addition, if I correctly guess an individual's KT, I should not be able to learn additional information or lock the individual out of her account by resetting their password. More research is needed to redesign the system.

What about Auroracoin? It did not use the government's central authority (bank account or mailing address) to authenticate new users and their supposedly registered KTs. Instead, Auroracoin had a list of names and dates of births with matching KTs and used Facebook profiles to determine whether a registration was valid. On April 22, 2015, Auroracoin ended its sign-up period for Icelandic residents to claim their coins [13], so I did not actually create Facebook profiles for any of the subjects to test. However, matching a Facebook profile's DOB and full name with a KT suggests vulnerabilities also. First, an impostor can set up a Facebook profile using name and DOB. If Auroracoin's system allowed unlimited (or even 100) attempts to guess the KT, the system would be vulnerable. On the other hand, if the impostor has the person's KT and makes a Facebook page for the person, then the system would also be vulnerable. Thus, a system which defers to private third-party services such as Facebook Connect presents further challenges as it creates a slippage between the use of the KT as a unique identifier and in itself an authenticator.

These findings strongly encourage further studies on the design of online systems that use national identifiers as authenticators, either centrally through a governmental system, or indirectly through third-party identity services.

References

1. Watson I. A Short History of National Identification Numbering in Iceland. Bifröst Journal of Social Science 4. 2010. http://bjss.bifrost.is/index.php/bjss/article/view/63

2. Þjóðskrá Íslands ID Numbers. Web. September 25, 2015, http://www.skra.is/english/population-register/id-numbers/

3. Arthur C. Apple Pay: A New Frontier for Scammers. The Guardian. March 2, 2015. http://www.theguardian.com/technology/2015/mar/02/apple-pay-mobile-payment-system-scammers

4. Keizer G. FBI Probes for Source of Fraudulent Turbotax Filing Spike. Computer World. February 11, 2015. http://www.computerworld.com/article/2882990/fbi-probes-for-source-of-fraudulent-turbotax-filing-spike.html

5. Newman L. Another Day, Another Health Insurance Hack Affecting 11 Million People. Slate. March 18, 2015. http://www.slate.com/blogs/future_tense/2015/03/18/premera_blue_cross_health_insurer_hacked_11_million_financial_and_medical.html

6. Identity Theft/Fraud Statistics. Statistics Brain Research Institute. April 8, 2015. http://www.statisticbrain.com/identity-theft-fraud-statistics/

7. Íslendingabók. Web. May 6, 2015, https://www.islendingabok.is/

8. Skoch I. Iceland: Genealogy Database: The Book of Icelanders Tracks Lovers Ancestry. Huffington Post. October 26, 2011. http://www.huffingtonpost.com/2011/10/26/iceland-genealogy-database_n_1032621.html

9. ÍslendingaApp SES(Beta), version 1.1, Android 2.2 and up. Sad Engineer Studios. 2014. https://play.google.com/store/apps/details?id=is.ses.apps.islendingaapp&hl=en

10. Odinsson B. Auroracoin. Auroracoin.org. Web. April 27, 2014, http://www.auroracoin.org

11. Female Names. January 1, 2014. Statistics Iceland. Web. September 25, 2015. http://www.statice.is/?PageID=1181&src=https://rannsokn.hagstofa.is/pxen/Dialog/view.asp?ma=MAN11111%26ti=Female+names+1+January+2014++%26path=../Database/mannfjoldi/NofnKvK/%26lang=1%26units=Number,%20Frequency

12. Male Names. January 1, 2014. Statistics Iceland. Web. September 25, 2015. http://www.statice.is/?PageID=1181&src=https://rannsokn.hagstofa.is/pxen/Dialog/view.asp?ma=MAN11101%26ti=Male+names+1+January+2014+++++%26path=../Database/mannfjoldi/NofnKK/%26lang=1%26units=Number,%20Frequency

13. Remains of the Premine Burned: Auroracoin. Web. May 6, 2015. http://auroracoin.is/EN/index.php/2015/04/22/remains-of-the-premine-burned/

Authors

Gili Vidan is a graduate student at the Department of the History of Science at Harvard. Her research interests lie at the intersection of technology, information, and constitutionalism. Her work employs STS analytical frameworks to interrogate topics such as online identity and authentication, cryptocurrencies, and cybersecurity. Before joining the History of Science department, she completed a MSc in Social Science of the Internet at the Oxford Internet Institute, where her thesis examined the social and material infrastructure of Bitcoin. She holds a BA in Social Studies with a secondary in Computer Science from Harvard College.

Editor: Shelia Jasanoff

Citation

Vidan G. Identity as a Service: Iceland's Kennitala and the Convergence of Identifier and Authenticator in Online Third Party Applications. *Technology Science*. 2015092902. September 29, 2015. http://techscience.org/a/2015092902

Data

Under review for data sharing classification. Data release available October 19.