TRUSONA CONFIDENCE SCORE

CALCULATING RISK TO INSURE ONLINE AUTHENTICATION AND IN-PERSON IDENTITY-PROOFING

BY ORI EISEN
FOUNDER AND CEO, TRUSONA

TRUSONA

INTRODUCTION

The purpose of this document is to establish a risk profile for different in-person identity proofing and authentication methods.

Until the methods are mapped to a confidence score commensurate with their risk, the Identity-as-a-Service (IDaaS) and Customer Identity Access Management (CIAM) industries will not be able to make federated identities a commercially viable business.

This paper will first explore the options available for identity proofing to assign a confidence score regarding the true person on the other end of an internet transaction. These are known as Levels of Assurance (LOA).

The second part of the paper will examine options for remote authentication of users after they provide a specific credential (soft/hard token), as well as look at the technologies involved in this process.

By determining an Identity-Proofing Confidence Score and a User Credential Confidence Score the Trusona Confidence Score can be calculated.

IDENTITY-PROOFING

As the name suggests, identity proofing is a method of establishing one's identity with the highest level of scrutiny.

We have been exposed to identity theft since the dawn of time, even in the Bible story of Jacob and Esau. When Jacob poses as Esau – "the voice is the voice of Jacob, yet the hands are the hands of Esau" – we witness the first documented identity theft.

Today, we most commonly use government-issued IDs to help identify who is who. Government-issued IDs are considered a commercially viable way to establish identity for most use-cases: entering a country to visit, applying for a job, showing that you are a licensed driver, etc. Nevertheless, not all government-issued IDs are created equal, and different types of IDs shouldn't be assigned the same confidence score or commensurate risk profile.

A driver's license can be obtained if you come to the DMV with your birth certificate. However, many online counties and recorder offices will provide anyone a copy of your birth certificate for $12.

So in theory, a criminal could pretend to be anyone once they obtain a birth certificate. This is a sad reality, as the birth certificate has no means to authenticate that an adult person is linked to it. The footprints of the baby will surely not match the adult. Further, there is no DNA-based way to link the person holding the original or a copy to this baby. Ultimately, there is really no way to know for certain that someone is who they say they are.

Once you think through this loophole, you realize that any government-issued ID is, at best, counting on the fact that no one is trying to cheat.

That being said, to attempt to truly know a person is who they say they are, we need something to set the bar as high as possible, knowing nothing is perfect.

Social Security Card
A social security card – printed on paper with no security features – is going to set a low bar.

Driver's License
A driver's license is the next level up, as it is printed on a plastic card and has security features that are both overt and covert (e.g. ink visible only under black light).

Passport
The next level is the passport, as it is printed on specialty paper and is bound in a booklet, and also uses security features that are both overt and covert (e.g. ink visible only under black light).

However, the most difficult feature of a passport to counterfeit is the NFC/RFID chip embedded in it, which contains the person's identity information. This chip is denoted by an e-passport symbol is on the cover.

E-passports have been in use since 2006 and most countries around the world issue them. The passport is made in layers, which include government printing of the booklet and state department issue of the chip and its cryptographic seal.

THE IDENTITY-PROOFING DOCUMENT CONFIDENCE SCORE

These are the maximum confidence scores for IDs:

- Social Security Printed Card = 20%
- Driver's License = 40%
- Passport/Green Card = 80%
- E-passport = 100%

Why are e-passports ranked at 100 percent? These have a unique security feature, which allows it to "Prove" authenticity beyond a shadow of a doubt. The rest of the documents, while still hard to counterfeit, cannot be validated without trusting the public notary, which is not always at hand.

THE IDENTITY-PROOFING PRESENTATION CONFIDENCE SCORE

We use a zero to 100 percent scale to reflect identity proofing confidence and the document security features used in it.

We use the terms Know, Show, Present and Prove to denote the different ways a document is presented and examined.

For example, a U.S. Passport with an NFC chip in it:

1. **Know** – A person knows the passport number, and/or any other information of this passport. The person can enter this information by typing it on a website, and/or say the information over the phone.
2. **Show** – A person shows the passport and its MRZ information via camera scan on a mobile phone, or video chat. Document could still be a good counterfeit.
3. **Present** – A person presents their passport in-person to an authorized agent. The agent can inspect the passport visually and also can scan the MRZ line in-person.
4. **Prove** – A person presents their passport in-person to an authorized agent. The agent is equipped with technology to prove beyond any doubt that the document is not a counterfeit.

The confidence scores for each are:
Know = 20%, Show = 40%, Present = 80%, Prove = 100%

THE IDENTITY-PROOFING CONFIDENCE SCORE FORMULA

Identity Proofing Confidence (IPC) is one number determined by the combination of documents used and how they are presented in the authentication process.

IPC = presentation confidence * document confidence

DOCUMENT CONFIDENCE	PRESENTATION CONFIDENCE	IPC %
Social Security Card = 20%	Know = 20%	20% * 20% = 4%
Social Security Card = 20%	Show = 40%	20% * 40% = 8%
Social Security Card = 20%	Present = 80%	20% * 80% = 16%
Social Security Card = 20%	Prove = 100%	20% * 100% = 20%

DOCUMENT CONFIDENCE	PRESENTATION CONFIDENCE	IPC %
Drivers License = 40%	Know = 20%	40% * 20% = 8%
Drivers License = 40%	Show = 40%	40% * 40% = 16%
Drivers License = 40%	Present = 80%	40% * 80% = 32%
Drivers License = 40%	Prove = 100%	40% * 100% = 40%

DOCUMENT CONFIDENCE	PRESENTATION CONFIDENCE	IPC %
Passport = 80%	Know = 20%	80% * 20% = 16%
Passport = 80%	Show = 40%	80% * 40% = 32%
Passport = 80%	Present = 80%	80% * 80% = 64%
Passport = 80%	Prove = 100%	80% * 100% = 80%

DOCUMENT CONFIDENCE	PRESENTATION CONFIDENCE	IPC %
E-Passport = 100%	Know = 20%	100% * 20% = 20%
E-Passport = 100%	Show = 40%	100% * 40% = 40%
E-Passport = 100%	Present = 80%	100% * 80% = 80%
E-Passport = 100%	Prove = 100%	100% * 100% = 100%

You could expand the formula to add additional factors, such as where the identity proofing took place (at an office, a user's home, in a park, etc.). You can also add the experience of the public notary inspecting the documents, or variables regarding the relationship of the user to the public notary (never met before, employer/employee, friend since childhood, jailbirds, etc.).

We assume the public notary is trained to look for forged documents, is not a rogue and is provided with technology to inspect the document to a "Prove" level. These conditions can only be carried out in person—not via video, telephone call or the Internet. For simplicity, however, in this paper we will ignore these variables.

THE USER CREDENTIAL CONFIDENCE SCORE

After we know the user's true persona, we provide them a credential. The quality of this credential is directly tied to our ability to know with confidence that this is the user on the other end of the transaction.

Let's imagine a situation in which four users are identity proofed with an e-passport to the level of "Prove" by validating the NFC chip. Our IPC would be e-passport (100 percent) * Prove (100 percent) = 100 percent level of confidence.

- User 1 receives a username/password as his or her credential.
- User 2 receives a QR code to scan each time they authenticate.
- User 3 receives a one-time passcode (OTP) token that changes passcodes every minute.
- User 4 receives a biometric fingerprint.

Much like each document has a confidence score, each user credential has a confidence score. Username and password is going to set the lowest bar, as that information could be guessed, brute-forced, phished by social engineering, stolen via malware, etc.

Surely, we can establish that giving a biometric reader is far superior to a user name and password.

While each attack vector has its own probability, we will assume the attacker is a nation-state actor with the ability to carry out sophisticated attacks.

What if the nation-state places malware on the device used to connect the biometric reader to siphon the session data and replay it later?

Any set of user credentials will allow an attacker to replay them and masquerade as the user.

In the case of OTP tokens, most are valid for one minute, and the attacker can open another session with the same keys unbeknownst to the user.

Replay, or replay detection, is therefore another critical factor in the confidence we place in the user credential. Practitioners call this feature Anti-Replay.

Maximum confidence scores for credentials are as follows:

- User name and password = 20%
- QR code = 40%
- OTP Token = 80%
- Biometric Reader = 100%

CREDENTIAL CONFIDENCE	ANTI-REPLAY PRESENT	UCC %
Username/password = 20%	No Anti-Replay = 20%	20% * 20% = 4%
Username/password = 20%	Anti-Replay = 100%	20% * 100% = 20%

CREDENTIAL CONFIDENCE	ANTI-REPLAY PRESENT	UCC %
QR code = 40%	No Anti-Replay = 20%	40% * 20% = 8%
QR code = 40%	Anti-Replay = 100%	40% * 100% = 40%

CREDENTIAL CONFIDENCE	ANTI-REPLAY PRESENT	UCC %
OTP Token = 80%	No Anti-Replay = 20%	80% * 20% = 16%
OTP Token = 80%	Anti-Replay = 100%	80% * 100% = 80%

CREDENTIAL CONFIDENCE	ANTI-REPLAY PRESENT	UCC %
Biometric Reader = 100%	No Anti-Replay = 20%	100% * 20% = 20%
Biometric Reader = 100%	Anti-Replay = 100%	100% * 100% = 100%

THE USER CREDENTIALS CONFIDENCE SCORE FORMULA

User Credential Confidence (UCC) score is one number determined by which credential is used and whether it includes Anti-Replay.

UCC = user credential confidence * anti-replay

THE TRUSONA CONFIDENCE SCORE (TCS) FORMULA

The components in the formula are comprised of both the level of identity-proofing confidence (IPC) and the level of user credential confidence (UCC) used to authenticate. By combining these scores, Trusona created the Trusona Confidence Score (TSC = IPC * UCC) so all authentication methods can be measured against a standard criteria.

Trusona Confidence Score = identity proofing confidence * user credential confidence

For example, an E-Passport presented in-person yields an Identity-Proofing Confidence score of 100%. Likewise, biometrics with anti-replay technology provides a User Credential Confidence score of 100%. Thus, the Trusona Confidence Score is the highest level of certainty possible of 100%. The Trusona Confidence Score can then be used to calculate the level of insurance a transaction may receive.

CONCLUSION

The need for better authentication is clear and growing. Practitioners can self-assess their identity confidence score like an insurer would, and measure their exposure.

This calculation allows organizations to determine the level of risk associated with current practices and what actions are needed to truly enhance online security.

By mapping authentication methods to a confidence score commensurate with risk, the Identityas-a-Service (IDaaS) and Customer Identity Access Management (CIAM) industries can balance customer experience with security and federate identities in a commercially viable way.

TRUSONA

info@trusona.com | **trusona.com**