The Trusted Identity Platform

Identity as the Root of Trust

Michael Frendo

Google Play Store, Amazon, Netflix, Twitter, FaceBook, Walmart etc are all common destinations for hundreds of millions of people, as are personal banks, credit card sites and more. In fact the average US resident has between 200 and 300 internet destinations that they log into. In most cases, these destinations maintain their own database of users and by extension some measure of identity. For fraudsters and other malevolent players, these destinations are both targets and opportunities. They are targets as rich sources of personal information that can be used to commit crimes like identity theft or credit card fraud. They are opportunities because most sites do not require or use any kind of true identity validation. This allows bad actors to create fake identities for a wide range of malevolent activities from theft to manipulation for opinion.

A similar situation is manifesting itself in government support for its citizens. The drive to increase efficiency, provide more timely service and more recently to deal with the effects of a pandemic is driving government services to move to the Internet at an accelerating pace. The missing link is a common identity management and verification methodology. Government agencies create their own individual identity management systems for services like the DMV, taxation, business registration, unemployment and in many states dozens of others. This is compounded by services that are less direct like K-12 education and post-secondary institutions, cities and counties.

None of this should be surprising. The internet was deliberately created as a distributed anonymous network. It was never meant to have central control or restrictions on access. It is this very aspect of the technology that enabled hundreds of thousands of entities to create technology and to grow the network and services in a way not previously possible. Yet even in the early days of the internet, it was recognized that access for many things needed to have more formality and control. The userID and password have also been around almost since the beginning but this was always believed to be “temporary” until a better methodology for identity and authentication was possible.

Much progress has been made in the last 25 years. The continued growth of the Internet and connected technologies (now popularly referred to as IoT) have enabled new and better ways to perform both identity verification and authentication. Physical IDs can be scanned with high resolution cameras and compared to live human 3D images captured. Real time checking of trusted databases (like DMVs and Passport databases) can be used to verify the ID is valid and the picture has not been doctored. The ability to move passed the userID and password is now here … finally.

Yet, this is not enough by itself. Moving sensitive personal information safely and effectively across the network must also be addressed. Sharing only what must be shared and no more must be enabled and enforced to ensure privacy. A well designed identity verification and authentication system in and of itself is an important building block but must be combined with a robust network solution to have the impact needed.

The question of multiple identity databases and methodologies must also be considered. Each database (or data lake) represents another target for the malevolent actor. Separate data lakes also represent an almost impossible task of keeping data up to date and synchronized. Separate data lakes also necessarily store data that is not needed for the function but only needed to help ensure authentication of the user. The question arises, “where is truth in identity?”.

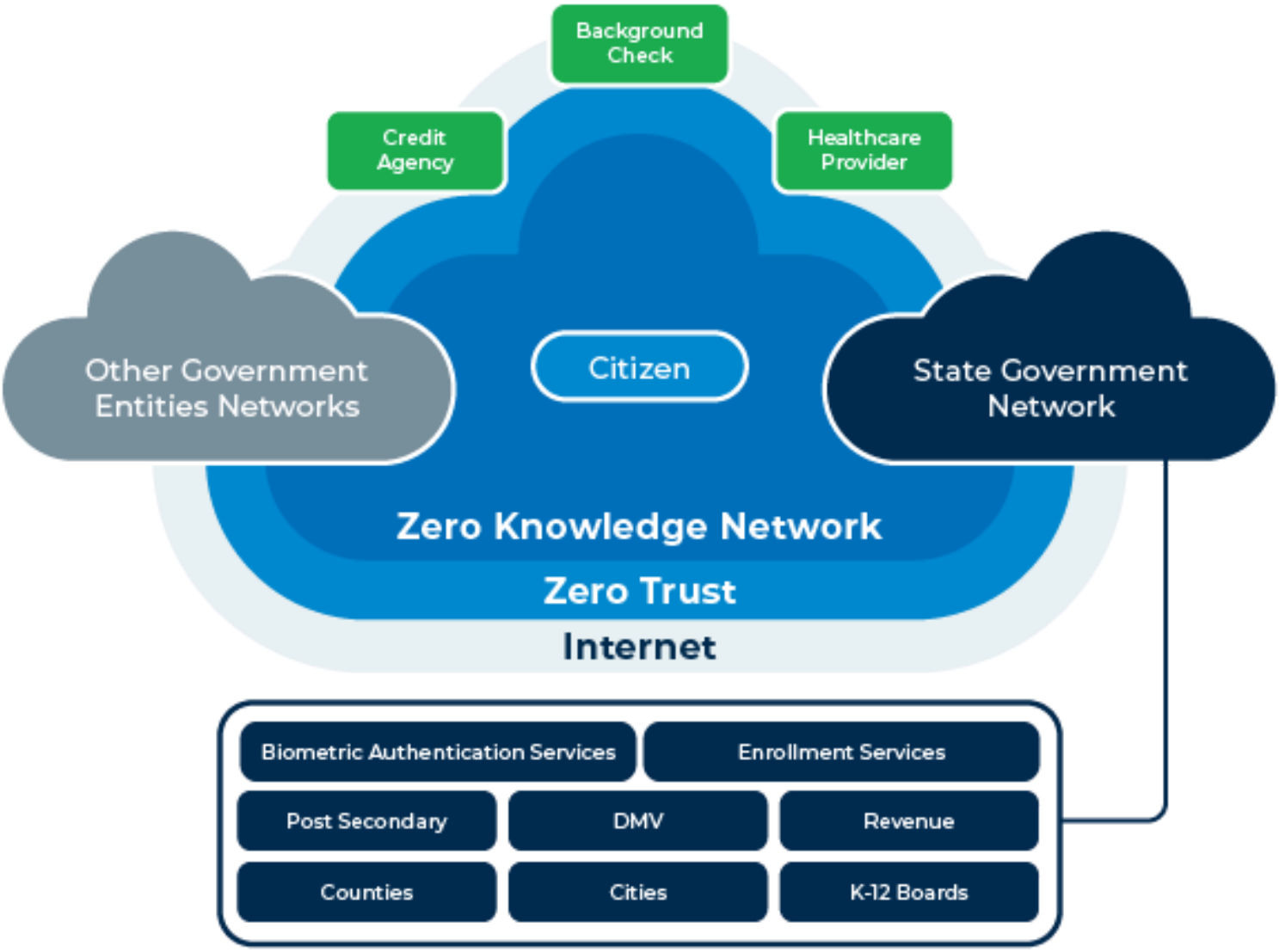
Fortunately we have many of the other building blocks to lean on already. DMV databases, passport databases, terrorist watch lists, credit reporting agencies, and background check agencies all exist today. All of these can be employed as building blocks for a more customer/user/citizen based identity management and authentication system.

The key is to knit together a system of verifiers, and agencies and citizens in a highly secure, privacy preserving identity network. This network must have the following attributes:

- Highly secure actors (verifiers, user agencies) accomplished by building a zero trust network. Every element must be verified to accomplish this.
- Privacy preserving communications where only the sender and receiver of personal data have access to the information. Even the network builder/operator should not have access to the data.
- The ability to prove certain attributes about a citizen without sharing those attributes. A very simple example is proving age of majority without sharing birth date. This is commonly known as a zero knowledge proof.
- Trusted verifiers like government agencies or credit bureaus that are integrated into the zero trust environment.
- Biometric verification and authentication systems that represent something that cannot be stolen or broken by algorithms.
- The elimination of redundant data bases or lakes.

At the core of this network is the individual citizen. Empowered by a verifiable and biometrically authenticatable identity, the citizen is able to interact with all agencies and enterprises securely and privately. As important, a non-verifiable and biometrically authenticable actor cannot.

The figure below depicts what a high level zero trust, zero knowledge network would look like for this approach.



This represents a subset of all the players that could be involved. It is in fact scalable to any number of agencies, any number citizens and any number of interested parties. Indeed, enterprises might also want to register for verified identity as a service should the state level players take this on to solve internal identity management.

Some important notes to consider:

- All communications between the identities depicted (and others) takes place over the zero trust, zero knowledge network

    - zero trust creates the first level of encryption to protect data on the Internet (first level of encryption)
    - communication between the citizen and all other entities connect on the zero knowledge network are not decipherable with in the zero trust network (second level of encryption)
    - zero knowledge can be extended to any actor in the network for example a contact center agent.
    - The same is true for communications between the entities
- Enrollment is achieved with a level of trust as required by the State. It can include any or all of the following
    - Facial biometric
    - Fingerprint
    - Voice print
    - Credit check
    - Background check
    - DMV Dip
    - Passport DIP
    - ....
- The DMV and other state checks are not limited to the state requesting verification for enrollment. Access to hundreds of government entities and state governments worldwide is available, as well as thousands of government ID documents.
- Biometric authentication (through Oauth or SAML or proprietary techniques) makes a central authentication service possible for all government agencies and potentially for enterprises as well
- Orchestration of services (while not depicted) provides the rules engine for a wide array of potential applications

In summary, the advent of powerful personal computing technology, combined with the sensors available on mobiles and (at least partially) desktop or laptop, has made it possible to create far more robust identity enrollment and authentication systems. What is missing in these is a robust, consistent and more user/citizen friendly network to bring it home.