Voatz Whitepaper (Draft)

Remote Digital Identity

Technology for Mobile Voting & Beyond

Abstract

The means to reliably establish the identity of citizens residing outside of their election jurisdiction has been an unsolved problem since the earliest days of elections.

In 2017, the National Institute for Standards and Technology (NIST) published SP 800-63-3 "Digital Identity Guidelines" for federal agencies seeking to improve the convenience of providing digital services to their constituents while maintaining the security of their IT infrastructure – problems faced by every election official. This paper "translates" the NIST technical guidelines for an audience of non-technical election officials who seek greater security in election administration and to improve the convenience to voters whose circumstances effectively prevent them from voting in person or by mail.

This paper is the first of a technical series that explains the security-related concepts of the Voatz mobile voting channel – the nation's first mobile voting system[i] used in a federal election.

Part 1 reviews the general concepts of "remote digital identity" as outlined in the National Institute of Standards and Technology (NIST) Digital Identity Framework (SP 800-63-3),[1] as well as how Voatz integrates those security concepts into a new mobile voting channel.

Part 2 describes the process to conduct an independent, end-to-end post-election audit of voter-verified ballots submitted remotely while preserving voter anonymity.

Part 3 examines the role of a permissioned blockchain and describes how Voatz employs open source blockchain software to secure the aggregate vote, to enable end-to-end post-election audits and to enable credentialed organizations to independently audit elections.

Part 4 relates the significant investments in accessibility being made by Apple and Google to voting securely on a smartphone.

Part 5 outlines the security aspects of modern smartphones (including their built-in biometric capabilities), the role of secure, worldwide software distribution platforms, and the accessibility, usability and privacy features that have made smartphones the fastest growing technology in history.

Remote Digital Identity: Technology for Mobile Voting

Overview

The means to reliably establish the identity of citizens residing outside of their election jurisdiction has been an unsolved problem since the earliest days of elections. Attempted solutions have, at best, distorted election administration – making elections more costly, more manual and more time-consuming – and at worst, have disenfranchised remote voters with logistical and bureaucratic hurdles.

> "Our study reveals that the voting rate of Americans living abroad would have increased from 7% percent to 37.5%, if overseas obstacles to voting were removed."
>
> David Beirne, Director
> Federal Voting Assistance Program
>
> FVAP.GOV
> FEDERAL VOTING ASSISTANCE PROGRAM

The result: The U.S. trails most developed countries in voter turnout[ii], military and overseas civilian voter participation remains extremely low at 7%[iii] and people with disabilities continue to face barriers with voting rates at 6-10% below the general population[iv].

Over the past decade, election officials have struggled to find a solution to enable registered voters, regardless of their location, to securely receive, mark, verify and submit their ballot in a way that satisfies the legitimate concerns over security and rigorous auditability. Voatz believes that solutions to increasing voter participation have largely been stymied by the absence of a clearly articulated technical vision that balances rigorously vetted security with convenience and usability for all voters.

The rest of this paper describes a Remote Digital Identity framework that was developed by the National Institute for Standards and Technology (NIST) and published in 2017. This framework provides technical guidelines for federal agencies seeking to implement digital identity services that cover identity proofing and authentication of users (such as employees, contractors or private individuals).

Voatz has adopted the NIST framework to integrate new technologies such as the biometric capabilities and accessibility features of smartphones, secure communications over the Internet[v] and digital ledger technology (blockchain) so that state and local election jurisdictions can provide significantly enhanced security while improving convenience to voters of all abilities.

This paper addresses the following identity-related security issues. Specifically, how to:

- Ensure that only registered voters can become remote voters,
- Establish the authenticity of credentials presented remotely,
- Confirm that the remotely presented credentials belong to a real person,
- Prevent a credentialed person from casting their ballot more than once,
- Prevent ballot access to remote voters who have not been biometrically authenticated.

Remote Digital Identity

Remote digital identity presents difficult technical challenges because this process involves proofing individuals over an open network from a user-owned device. Fortunately, detailed guidelines exist[vi] and are widely used in other critical infrastructure industries. These guidelines can be used to inform developers and independent testing organizations of the best practices to ascertain the identity of voters while respecting their privacy and balancing their need for convenience, accessibility and ease-of-use. These guidelines introduce four important concepts:

Digital identity: The unique representation of a registered voter engaged in online voting.

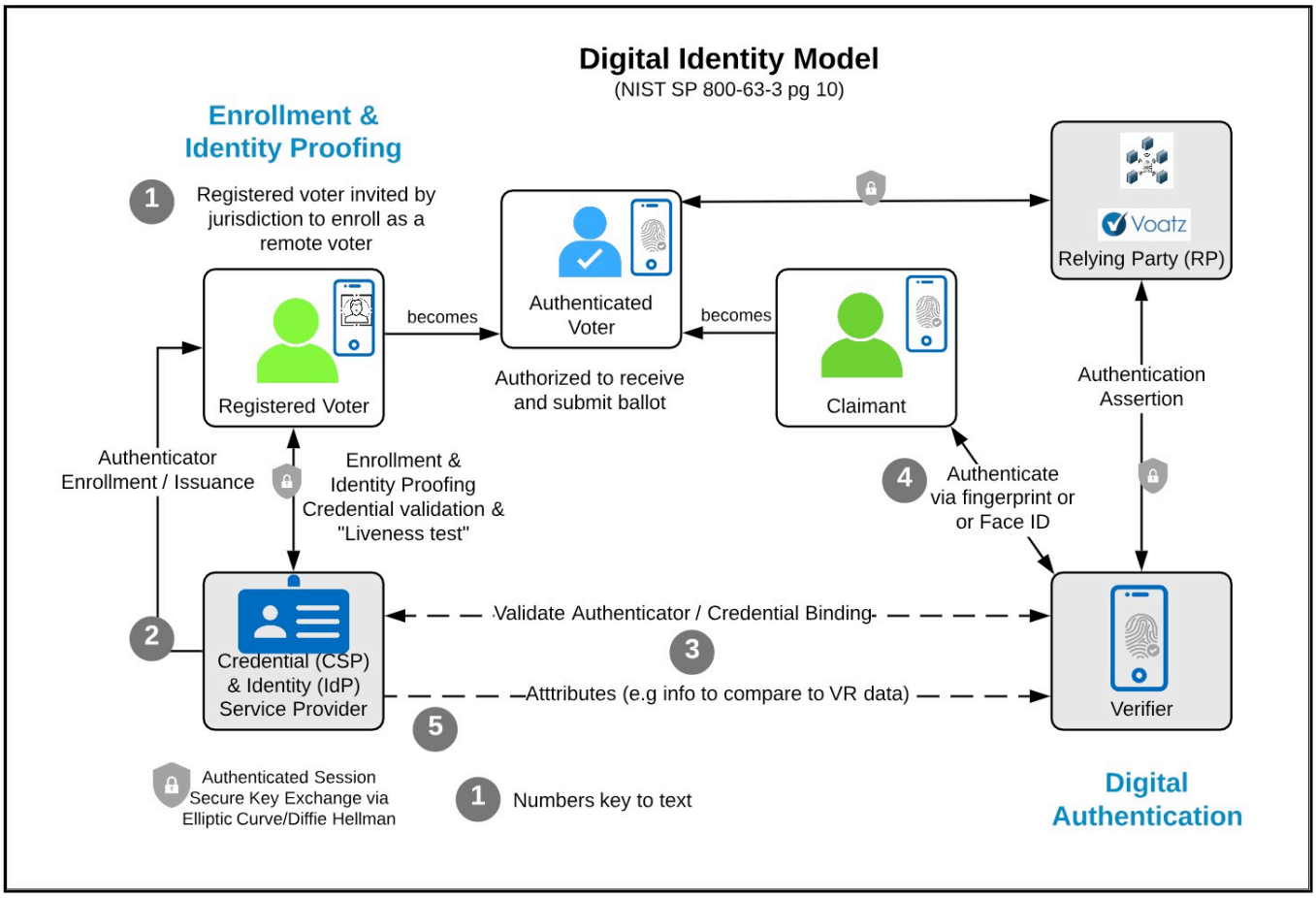
Remote identity proofing: Establishing that a registered voter is who they claim to be through a three-part verification process described below.

Binding: A biometric process that ties a voter to their device to prevent double voting.

Authentication: Confirmation that, at the time of voting, the person requesting ballot access is the same person whose identity was proofed. Once authenticated, the voter is granted *authorization* to access their blank ballot and to submit their voted ballot.

The Process of Remote Digital Identity (Translated for Elections)

The graphic below has been copied from the NIST publication SP 800-63-3 (page 10) and annotated with terms familiar to election officials. Refer to this graphic to see the relationship between the services outlined below that comprise digital identity.



Remote Enrollment, Identity Proofing and Binding

Enrollment, identity proofing and binding comprise a process that occurs episodically and is typically renewed when a government-issued credential expires, or the user acquires a new smartphone.

Remote Enrollment

The first phase of Identity Proofing begins with enrollment. Here the jurisdiction sends an email or letter inviting a registered voter to vote remotely. The correspondence contains instructions on how to configure their device to vote remotely and a means of authenticating the voter.

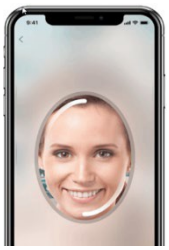
Enrollment ensures that only invited registered voters can vote remotely.

> Voatz integrates with the jurisdiction's voter registration system (VRS) to simplify the invitation process. The invitation contains instructions to download the Voatz smartphone application from the App Store (iOS) or Google Play Store (Android). When the user completes the process of identity proofing, they are confirmed as registered voters against the VRS. This process ensures that, even though anyone can download the Voatz smartphone application, only duly registered voters can use the application to access their ballot.

Remote Identity Proofing

In the second phase, the registered voter presents an approved government-issued photo ID (the "credential") to the jurisdiction. An authorized Credential Service Provider (CSP) verifies the validity of the government-issued credential. An authorized Identity Provider (IdP) performs a biometric test for "liveness." Identity validation is done by comparing the photo image of the remote person to the picture in the government issued credential. The secure communication between a relying party and third party CSPs and IdPs is done through the process called "federation" described below.

Credential Verification



Proof of "liveness"

Identity proofing answers the question, "Is this person who they say they are and does that person exist in the real world?"

> Voatz uses the smartphone's digital camera to capture an approved credential (i.e. driver's license, passport or government issued photo ID). The Voatz smartphone application integrates a third party CSP to perform both credential verification and "liveness" detection. Credential verification is a sophisticated process in which the CSP automatically examines the security artifacts of the voter's credential against their database of known credentials. Confirmation of "liveness" is performed biometrically by taking a video "selfie" where the voter is asked to nod their head and blink their eyes. Voatz has two options to perform the comparison of the video selfie to the photograph of the voter's credential: manually by Voatz personnel during the small pilots of governmental elections and automatically during a relatively large election by requiring agreement between two competing facial recognition services. When there is not agreement, an authorized human makes the decision which may include a video chat with the requesting person (e.g. via Skype). Biometric data is retained only as long as it takes to verify the identity of the registered voter in the real world.
>
> Note: There may be a delay in comparing the video selfie to the voter's credentials; until then the Voatz application will indicate a "pending status." The voter cannot open their ballot until notification of a successful resolution of identity is received by the smartphone application.

Binding

Binding is the final phase of identity proofing. Here the user biometrically binds the identity-proofed person to their smartphone. Binding prevents an identity-proofed person from voting on another device and prevents another person from voting on the smartphone that went through the identity-proofing process. For security reasons, it is critical that this step be done in the same session as the identity proofing step.

Binding prevents a remote voter from casting a ballot more than once and enables secure authentication (see below).

> Binding is achieved when the Voatz smartphone application requests the user to re-authenticate themselves in the same way they did to gain access to their phone – e.g. via fingerprint, face ID or PIN.

References

Section 4.4 of NIST SP 800-63A[vii] (Enrollment and Identity Proofing) provides the technical requirements for identity proofing of voters who wish to gain *remote* access to government services like voting in federal and state elections from overseas or from home as with voters constrained in their mobility. It also provides informational and normative guidelines to educate developers and independent testers of the procedures required for secure, remote identity proofing.

Authentication and Lifecycle Management

Authentication

Voter authentication occurs in every election; it is unlike identity proofing which is episodic. Authentication is central to the process of associating the device to the identity of a remote voter just prior to their act of voting – but not *how* they voted. Authentication is performed by verifying that the voter possesses at least one method, called a "valid authenticator," of ensuring that their identity can be confirmed at the time of voting. Devices with biometric capabilities can serve as a valid authenticator.

> Voatz uses the smartphone as the "valid authenticator." In the Voatz application, authentication is requested twice in a voting session: once when the voter tries to open their blank ballot and again when the voter submits their voted ballot. Authentication – via fingerprint, face ID or PIN – provides a registered and identity-proofed voter with the *authorization* to access their blank ballot and the *authorization* to submit their voted ballot. Voatz carefully follows the required protocols for certificate key exchange (using Elliptic Curve/Diffie-Hellman) and approved cryptographic encryption (using AES 256). These standards provide for secure communications between the application and the voter.

Authentication provides a reasonable assurance that the person who voted today on their smartphone is the same person who voted previously on the same smartphone.

References

Section 4.4.2 of the document, NIST SP 800-63B[viii] (Authentication and Lifecycle Management), provides reference and normative information on remote Authentication Assurance Level 2. This technical guideline also requires that approved cryptographic and encryption methods be used to communicate between all parties – the application provider, the jurisdiction, any 3rd party Credential Service Providers, Identity Service Providers and the voter.

Federation

Federation is a process that allows for the secure conveyance of authentication and voter attribute information across networked systems. In a federated system, the Credential Service Provider (CSP) and the Identity Provider(s) (IdP), provide identity services to the application developer, called the Relying Party (RP). Federation requires relatively complex multiparty protocols that have subtle security and privacy requirements and require careful consideration.

Federation speeds progress by enabling "best-of-breed" technologies to be securely integrated into a solution.

> In the diagram on page 2, Voatz is the "Relying Party" (RP). Voatz contracts with 3rd party providers who provide credential validation and "liveness" detection. Federation, as adopted by Voatz requires that these firms adhere to the NIST 800-63-3 or ISO/IEC 30107-3 (Biometric presentation attack detection) guidelines. Voatz carefully follows the required protocols for certificate key exchange using Elliptic Curve/Diffie-Hellman (see endnote v) and approved cryptographic encryption methods (using AES 256). These standards provide for secure communications between independent service providers, the relying party, the voter and the jurisdiction.

References

The document, NIST SP 800-63C[ix] (Federation and Assertions), provides normative requirements to Credential Service Providers (CSPs), Identity Providers (IdPs) and Relying Parties (RPs) of federated identity systems.

Conclusion

Voatz believes that citizens deserve a system that allows them to vote safely, easily and with confidence that their vote will be counted, regardless of their circumstances.

Political parties spend hundreds of millions of dollars to "get out the vote," and yet in the 2016 Presidential Election:

- Only 56% of the voting-age population voted[x].
- Only 7% of citizens who live and serve abroad voted[xi];
- Only 43% of voters age 18-29 voted[xii].
- While 71% of those over age 60 voted[xiii], those politically active voters may face increasingly age-related disabilities that, over time, will make it more difficult for them to remain engaged in our democracy.

The above statistics are for presidential elections. Midterm participation rates are typically 20 percentage points below presidential election years and turnout in municipal elections hovers around 25% with some important mayoral races being decided by only 5% of eligible voters.[xiv]

Support for America's Election Officials: The Path to Progress

In elections, progress often comes when an election official is passionate about solving a problem, can visualize an end-to-end solution and can explain it in simple terms. At Voatz, we believe it is our job to supply those visionary election officials with a clear, practical, end-to-end technical solution to the problem and to support them with communication tools to help them build a case for change.

This paper is meant for election officials who seek background on the topic of Remote Digital Identity. It follows the guidelines for Digital Identity developed by the National Institute for Standards and Technology. These guidelines systematically address one of the election industry's thorniest technical problems – *how to establish voter identity remotely*. Specifically, we have described how:

1. *Enrollment* ensures that only designated registered voters can vote remotely.
2. *Identity proofing* answers the question, "Is the person who they say they are and does that person exist in the real world?"
3. *Authentication* provides a reasonable assurance that the person who voted today on their smartphone is the same person who voted previously on the same smartphone.
4. *Binding* prevents a remote voter from voting twice.
5. *Authorization* enables an authenticated voter to access and then to submit their ballot.
6. *Federation* speeds innovation by enabling "best-of-breed" technologies to be securely incorporated into an integrated mobile voting solution.

Finally, we hope this paper, and the others in this series, provide a rigorous framework that can elevate the current national discussion of the role of technology in elections.

Endnotes:

---

[i] See, "Under the Hood: The West Virginia Mobile Voting Pilot, at https://blog.voatz.com/wp-content/uploads/2019/02/West-Virginia-Mobile-Voting-White-Paper-NASS-Submission.pdf

[ii] See "U.S. Trails most developed countries in voter turnout," https://www.pewresearch.org/fact-tank/2018/05/21/u-s-voter-turnout-trails-most-developed-countries/

[iii] See "DOD Releases Study of U.S. Voters Abroad," https://www.fvap.gov/info/news/2018/9/12/dod-releases-biennial-study-of-us-voters-abroad

[iv] See American Association of Peoples with Disabilities, AAPD Statistics & Data https://www.aapd.com/advocacy/voting/statistics/

[v] See Cloudflare, "A Relatively easy to understand primer on elliptic curve cryptography" at https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/

[vi] See NIST SP 800-63-3 "Digital Identity Guidelines" at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

[vii] See NIST SP 800-63A "Enrollment and Identity Proofing," at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf

[viii] See NIST SP 800-63B "Authentication and Lifecycle Management," at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

[ix] See NIST SP 800-63C "Federation and Assertions," at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63c.pdf

[x] See "U.S. Trails most developed countries in voter turnout," https://www.pewresearch.org/fact-tank/2018/05/21/u-s-voter-turnout-trails-most-developed-countries/

[xi] "DOD Releases Study of U.S. Voters Abroad," https://www.fvap.gov/info/news/2018/9/12/dod-releases-biennial-study-of-us-voters-abroad

[xii] See "Voter Turnout Demographics – raw data" at http://www.electproject.org/home/voter-turnout/demographics

[xiii] Ibid

[xiv] See Fairvote, "Voter Turnout in the United States," at https://www.fairvote.org/voter_turnout#what_affects_voter_turnout_rates