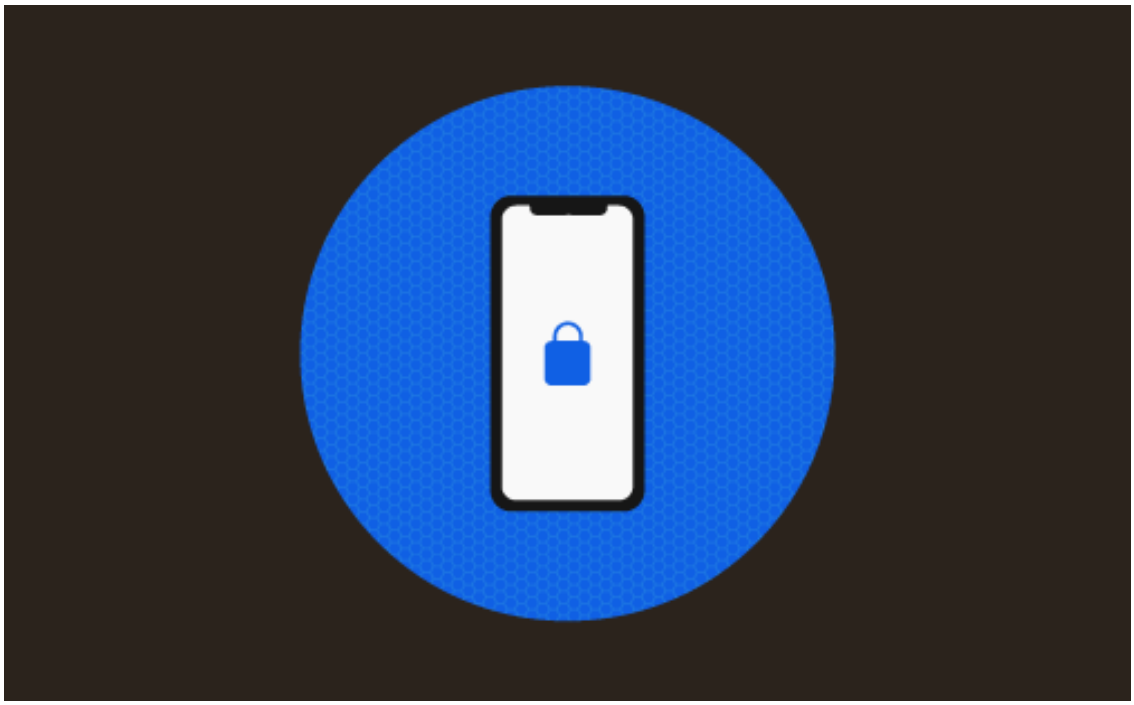
BLUINK LTD

eID-Me Privacy and Data Protection

Version 1.4

Prepared by: Larry Hamid, CTO



BACKGROUND

Identity theft is a growing problem that costs tens of billions of dollars annually to individuals and organizations. Massive data breaches provide the main source of Personally Identifiable Information (PII) for cybercriminals to carry out their identity theft operations. Unfortunately, these massive data breaches seem to show no sign of slowing down. In 2018, over one billion records were reported breached in the U.S. alone.

Date	Organization	# of Records	Type of Data
Jul 2018	Exactis	340,000,000	name, email, phone #, home address, relatives, and more
Nov 2018	Marriott International	327,000,000	name, address, phone #, email, passport #, date of birth, gender
Mar 2018	Under Armour	150,000,000	username, email, hashed password
Oct 2018	MindBody - FitMetrix	113,500,000	name, gender, email, phone #, photo, workout location, emergency contact, and more
Jun 2018	MyHeritage	92,283,900	email, hashed password
May 2018	T-Mobile	74,000,000	name, address, billing account #
Sep 2018	Facebook, Inc.	50,000,000	Still being determined
Apr 2018	Localblox	47,000,000	Aggregated data from publicly accessible sources
Oct 2018	Chegg	40,000,000	username, email, addresse, hashed password
Apr 2018	Panera Bread	37,000,000	email, addresse, phone #, loyalty account #

Top 10 data breaches in 2018. Source: Privacy Rights Clearinghouse

The centralized storage of massive amounts of PII creates huge targets for cybercriminals to attack. As long as such massive stores of PII continue to exist, data breaches will continue to occur, providing fuel for identity-related cybercrime. Since eID-Me is an identity solution, it necessarily manages sensitive PII. However, the way eID-Me handles this PII makes traditional data breach attacks ineffective against it.

A Different Paradigm

Privacy and data protection are core principles of the eID-Me identity solution. No centralized store of PII exists within eID-Me, which prevents it from becoming a massive target for cybercriminals. Operators of an eID-Me solution, whether a private company or a government entity, need not fear such massive attacks and the subsequent disclosures, costs, and damage to reputation that it causes.

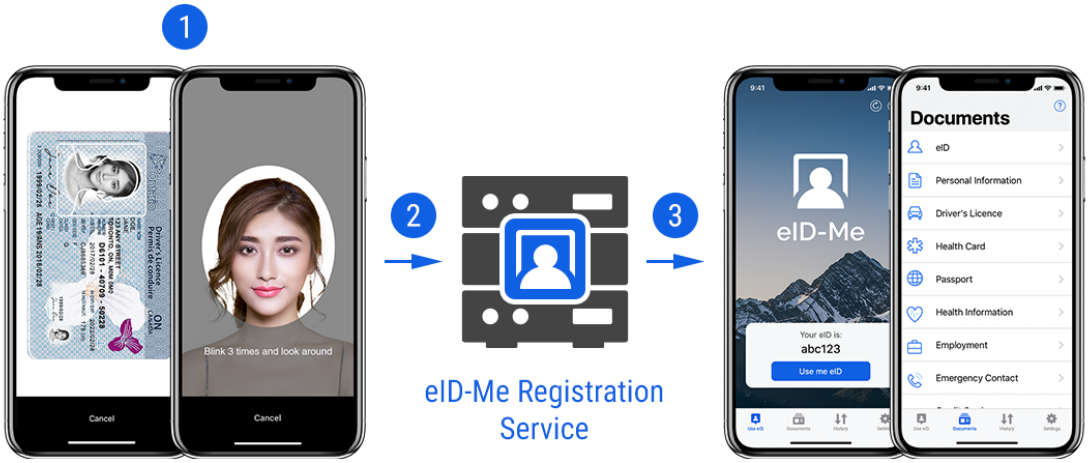
Individuals that use eID-Me also have peace of mind knowing that eID-Me does not host any of their personal information in a centralized data store. Instead, users are in possession of their PII, which is secured on their personal smartphones, and they are in full control of when and to whom their information can be released.

Relying parties can also reduce their exposure to data breaches if they leverage the eID-Me paradigm to reduce their footprint of stored PII data.

OVERALL EID-ME FLOWS

In order to fully understand the privacy and data protection within eID-Me, we must to look at eID-Me's workflows and how user PII is managed throughout each of them.

Registration and Identity Proofing



eID-Me Remote Registration and Identity Proofing

The first stage of the eID-Me identity solution is the process to register and obtain a digital identity. Referring to the above diagram, this process has the following steps:

1. Capture identity documents.
2. Submit PII for identity proofing.
3. Issue eID-Me identity to smartphone.

The user begins the registration process by submitting an email address to receive a registration code.

In step 1, a user captures identity documents and a selfie using the eID-Me smartphone app. This information is securely stored with strong encryption in the app. The app itself is protected with

smartphone authentication (a smartphone PIN, passcode, or biometric) to prevent others from viewing this information.

In step 2, the collected information is submitted to the eID-Me registration service to check the validity of the information and perform additional checks, such as biometric comparisons and location verification, to produce a Strength of Identity Proofing (SIP) score. If this score is too low to issue an identity, the submitted information is destroyed and steps 1 and 2 need to be partially repeated.

In step 3, once a sufficient score is attained, a digital certificate is generated for the eID-Me identity containing hashed values of the PII and an anonymous identifier. This eID-Me certificate and the corresponding PII identity claims are returned to the smartphone for secure storage. Once the identity has been installed on the smartphone, the PII on the registration service is destroyed. In all situations, the eID-Me registration service will only retain PII for a maximum of two hours to allow the issuance step to be completed.

During the short period of time required to issue an identity, the eID-Me registration service retains PII and strongly encrypts it with keys that reside in a hardware security module. Step 3 is the only time in which PII is ever stored by eID-Me outside of a user's smartphone, and this is only temporary.

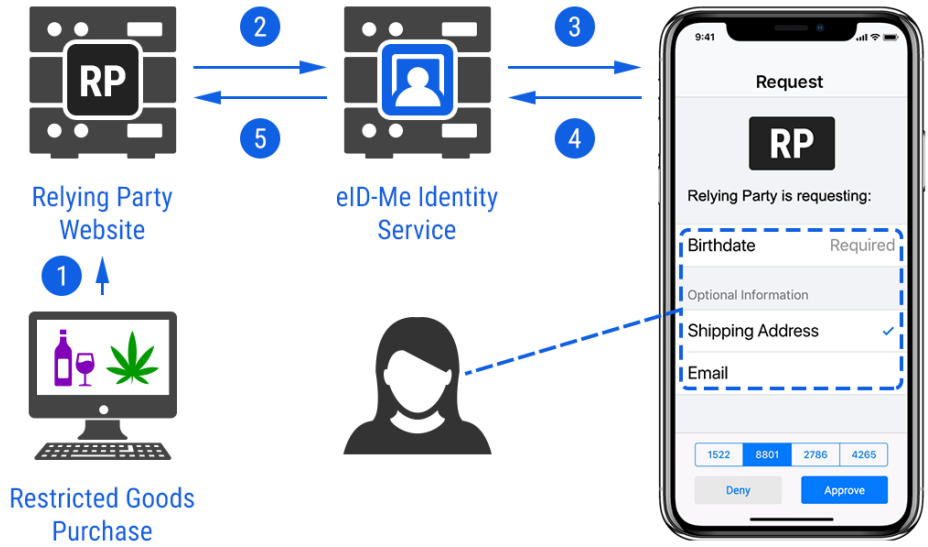
After issuance, the only data that is retained by the eID-Me service is the following:

- eID-Me anonymous identifier
- A smartphone token used for push notifications
- Smartphone public keys (for authentication and secure messaging to smartphones)

Online Usage

The online usage of eID-Me allows a user to interact with relying parties (websites). In most cases the eID-Me identity can be used as a strong authenticator for the user without passwords. No PII needs to be exchanged in such a transaction. This alone is a powerful feature of eID-Me as it removes the burden of storing usernames and hashed passwords, making relying parties less of a target for cybercriminals. The obvious benefits to individuals is that they no longer have to remember passwords.

Some other use cases require identity claims during a transaction. For example, a site that sells restricted goods such as alcohol or cannabis needs to verify the age of their customers. In this case, the relying party could request a verified date of birth from the user's eID-Me app. This flow is illustrated in the following diagram.



eID-Me online usage requiring identity claims

The steps numbered in the above diagram are the following:

1. User browses a website and initiates a transaction.
2. The relying party contacts eID-Me via a federation protocol (OpenID Connect or SAML).
3. The eID-Me Identity Provider sends an encrypted message to the user's smartphone.
4. After confirming the transaction, the result is digitally signed by the eID-Me identity.
5. After verifying the result, the requested claims are returned to the relying party.

To follow the PII through this flow, these steps will be described in more detail.

In step 1, the user sees that some PII is required (such as age verification) in order to complete the transaction. The relying party provides an option to use eID-Me to supply this information via a button.

In step 2, the user session is redirected to the eID-Me identity provider which in turn requests the user's eID-Me anonymous identifier.

In step 3, knowing the eID-Me identifier, the eID-Me identity service is able to lookup the user's smartphone token and encryption public key. It then packages up the request from the relying party in a secure message that can only be decrypted by the target user's smartphone. The smartphone receives the message and displays it for the user to view and confirm. The user clearly sees who the requestor is and which identity claims they are requesting. In this example, the relying party needs the user's date of birth. The user has the option of denying the entire request or deselecting any optional claims being requested.

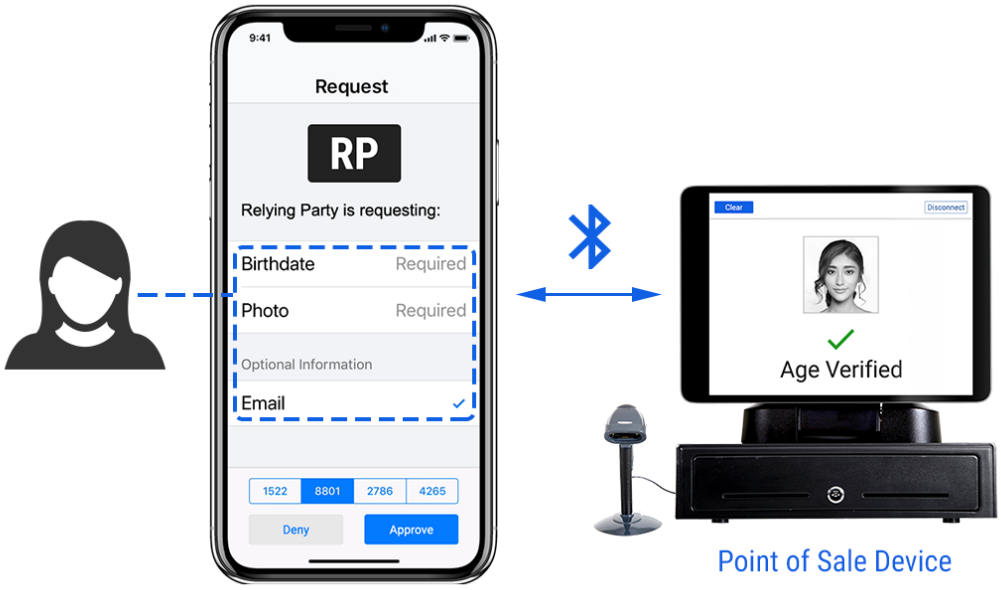
In step 4, the requested claims and the eID-Me identity certificate are packaged up into a response and digitally signed by the eID-Me identity private key. The eID-Me identity service verifies the digital signature, certificate, and the provided claims. If the claim has a hashed value contained within the certificate, it is checked to ensure that the value is correct.

In step 5, the result of the verification of the response from the smartphone is passed onto the relying party along with any requested identity claims that the user chose to release.

In this entire flow, no PII data is stored in any eID-Me service. Any PII that is sent from the smartphone is verified in memory before being passed on to the relying party. It is recognized that what a relying party does with PII, what information they retain, and how they protect it is beyond the scope of eID-Me. It is something that end users should be aware of whenever responding to transaction requests.

In-Person (Offline) Usage

eID-Me also supports transactions that can be performed in-person or face-to-face as illustrated in the following diagram.



eID-Me in-person (offline) usage

In in-person transactions, there is no eID-Me service involved. These transactions are performed directly between the user's smartphone and a host system (considered to be the relying party). Even though no eID-Me services are involved, the user experience is very similar to the online transaction use case. There are many possibilities for what the host system can be, including a Point of Sale (POS)

terminal at a retail store, a medical clinic check-in station, a police officer's smartphone, an automobile, or a home door lock.

Since no eID-Me services are involved in in-person transactions, any PII which is released by the user is only seen by the relying party's host system. As in the online transaction use case, the user should be aware that releasing information to a relying party takes it outside the control of eID-Me.

PRIVACY AND DATA PROTECTION

The previous discussion has disclosed where user PII exists in every eID-Me flow. Here we will discuss the privacy and data protection implications offered by eID-Me.

Security Token Model

It should be clear now that there is no centralized store of user PII in the eID-Me system (excluding relying parties). Instead, user PII is actually distributed and carried on the owner's smartphone. It is very similar to the "security token" model of a smart card, where data and keys belonging to an individual are actually carried by the individual in a module with hardware security. While smartphones are not smart cards, they are increasingly becoming equipped with hardware security mechanisms (secure elements, trusted execution environments (TEE), and secure enclaves (iOS)) that provide strong security for keys and cryptographic operations. eID-Me leverages hardware security to provide stronger protection of the stored user PII if it exists on the smartphone.

One of the desirable consequences of this model is that if a smartphone is ever lost or stolen, it is virtually impossible for an attacker to decrypt any eID-Me data stored on it, even if they were able to copy the data off of the smartphone. Furthermore, services such as "find my phone" allow a user to locate their smartphone and remotely reset it. This operation permanently erases any data on the smartphone and further adds to the peace of mind a user should have about their PII stored by eID-Me. Losing an eID-Me smartphone is much safer than losing a wallet of identity cards.

Distributed PII Data

The distributed nature of the PII data within eID-Me makes it very challenging for cybercriminals. There is no large target for cybercriminals to attack, eliminating the potential of a massive data breach. Instead, any attack which tries to obtain PII data from eID-Me must attempt to do it one smartphone at a time. This is a deterrent that should make eID-Me an unattractive target for cybercriminals.

Reauthentication

It was mentioned earlier that the eID-Me smartphone app and its data is protected by the user's smartphone authentication mechanisms. The app will automatically lock after a short period of inactivity, requiring the user to authenticate using their smartphone authentication method to gain access to the app.

However, even if the app is unlocked, there is an additional data protection mechanism that prevents a passerby from picking up the smartphone and accessing the PII stored within it. This mechanism is known as reauthentication. It is a property that can be set on any identity claim stored within eID-Me and requires the user to successfully verify themself using a smartphone authentication method before such an identity claim can be viewed or used in a transaction. For example, if reauthentication is enabled on a driver's licence number, then any attempt to use that identity claim in a transaction or view it in the app will require smartphone authentication first. eID-Me comes with default settings for reauthentication on a number of identity claims, but users can control these settings according to their own preferences.

No Tracking

While the eID-Me identity provider is involved in online transactions, it knows when relying parties are making requests, but it does not track any usage of individual eID-Me identities. No eID-Me identifiers or smartphone identifiers are kept in any transaction logs to ensure that privacy is respected. As a result, no correlation of which user is using what service can be made from any service logs.

Relying Parties

It is worth briefly discussing the opportunities that exist for relying parties that wish to adopt eID-Me. It is not just individuals that can benefit from the privacy and data protection of eID-Me. Relying parties can also benefit in a couple of ways. First, since no passwords are required for eID-Me transactions, the relying party can reduce its reliance on usernames and hashed passwords, making it a smaller target to attackers who try to steal and crack databases of passwords offline. This is the most obvious and immediate benefit that relying parties can gain.

Second, while eID-Me cannot control what identity information a relying party actually retains, the convenience of eID-Me presents an alternative to the traditional habit of storing user PII. Many online services store user data for convenience reasons. For example, having an individual enter their credit card information or shipping address every time they want to perform a transaction creates significant friction. This naturally drives relying parties towards storing more data than they actually need (or want), which makes them targets for cybercriminals.

eID-Me transactions enable any kind of PII to be requested and easily authorized for release by the user with simple touch gestures. For example, something as cumbersome as a shipping address can be

requested and instantly transmitted to the relying party with hardly any effort from the user. With this level of convenience, it is feasible for relying parties to consider not storing user PII at all.

FINAL REMARKS

The eID-Me solution is immune to the growing trend of massive data breaches of user identity information. Any relying party that accepts eID-Me identities will enjoy immediate benefit from strong authentication and the elimination of passwords. This is not only better for their customers (as it is more convenient and secure), but it also reduces a relying party's exposure to any data breach of customer usernames and hashed passwords.

Information that is either hard for a user to remember or inconvenient to type can be quickly and automatically transmitted in responses via simple smartphone touch gestures in an eID-Me transaction. This is not only convenient but offers better security for users since it avoids man-in-the-browser attacks.

The removal of friction in data entry enables a relying party to simply ask for user information when required. While it may be unavoidable in some business models to not store user PII, eID-Me's convenience offers a compelling alternative to creating large stores of PII for relying parties. This paradigm shift could finally give individuals and organizations a desperately needed advantage over cybercriminals.