Gemalto Presents: Digital Driver’s License — Security & Privacy by Design

As we continue to explore the possibilities enabled by a digital identity, it is important to establish a few fundamentals — particularly when it comes to security and privacy considerations. As a digital security company with decades of global experience protecting information, Gemalto has designed our digital driver’s license solution with both security and privacy at its core.

This quick reference document takes a look at our top three considerations and critical components when it comes to setting the standard for digital identity protocol and usage in the field.

Security

1. Seeing is not the same as verifying

When it comes to ensuring that a digital credential is valid and authentic, it’s important to make the distinction between performing a visual inspection and performing an actual verification of the credential data. Though it may seem like an easy, and somewhat natural, inclination to simply show someone a DDL displayed on a mobile device, it undermines the security benefits brought by a digital credential and opens the door to fraudsters. Creating a “realistic looking” digital ID is relatively simple; but creating a DDL with the underlying cryptographic keys and digital signature that would read as genuine upon digital verification is virtually impossible. In addition, you as the user lose the benefit of restricting your personal information to only the data required for the transaction if you simply show someone the image of your DDL on your mobile device. In fact, in the not-too-distant future, we may see DDLs evolving to the place where they have little or no visible representation of a physical credential. Doing so would ideally help to foster the behavior of digital verification in each and every scenario and would create a drastic reduction in identity fraud.

2. The issuer’s digital signature is the key

Validating a credential using digital authentication is actually doing two things simultaneously. First, it ensures the data being reviewed by the verifying party is accurate and reflective of the data on file with the issuing state’s driver licensing division. Second, it confirms the issuing entity’s digital signature or certificate is not only present on the DDL, but matches the value that is expected. The origin and authenticity of the digital signature can be verified by checking it against the Issuing Authority (IA) certificate found in the PKI [public key infrastructure] certificate management system. If a DDL is presented with a signature that does not match with the corresponding certificate of the IA, the credential can immediately be flagged as non-genuine or having been tampered with. This level of reliability and immediacy in affirming authenticity of a document with certainty is a tremendous advantage of digital ID.

3. Encryption and isolation matter

Naturally, encrypting the data associated with a digital credential is fundamental to ensuring security. This protection should extend beyond just secure storage on the mobile phone itself. Encryption should also be present at the point of origin and during transmission, so that all personally identifiable information (PII) is secure — whether at rest or in an active state. Furthermore, a DDL should be isolated in a secure container on a mobile device. This isolation prevents the co-mingling of data and provides layered security that doesn’t rely solely on the security mechanisms or protocol found in the operating system (OS) of the device. Unfortunately, operating systems are often huge targets for hackers and fraudsters largely because of their widespread use. Isolation ensures that your DDL is not subject to any potential vulnerabilities of the OS and is protected behind multiple layers of security.
One of the strongest benefits of moving from a physical credential to a digital credential is that the data found within that credential can now be dynamic. This is a tremendous advancement not only for the reliability and accuracy of information in the field, but also for the enhancement of user privacy. If data can be selected and segmented in a dynamic way, then it can be shared selectively at the discretion of the license-holder. When a verifying party — such as a pharmacist — needs to confirm your name and date of birth for a prescription pickup, for example, you can choose to share only these data elements, keeping all unnecessary information confidential. The ability to selectively disclose driver’s license data is the first step in limiting exposure of your personal information at a time where privacy concerns and data misuse are reaching new levels.

Not only should the license-holder choose what data they are sharing, but they should also be in control of deciding when they want to share it and with whom it is shared. That’s why a DDL transaction is always triggered by the user. There are no broad spectrum pings coming across to request your data in a convoluted manner (as can sometimes be the case with other forms of data sharing). DDL verification of any kind can only occur when the rightful owner of the mobile phone launches the DDL application, authenticates themselves via PIN/biometrics, and selects the option to perform a verification — such as when attempting to prove their age, at a TSA checkpoint, or interacting with law enforcement. Without those steps, the data found within the DDL application is completely inactive and inaccessible by third parties. If only all of our personal data in other areas could remain securely hidden until we choose to say the magic words and reveal them to a trusted party.

Once a verification scenario has been triggered, there are two additional components that should be adhered to in order to maintain user privacy. First, the verification should be performed offline. This means that no geo-location tagging or activity tracking of the verification transactions a DDL has logged can occur. In fact, a DDL verification doesn’t require any mobile or WiFi connectivity whatsoever. The actual authentication of the credential occurs between your device and the verification device — not in the cloud or after logging an entry on a DMV server somewhere. This ensures that verifying parties and your state’s licensing division have no more information on your personal activity with a DDL than with a physical driver’s license. Unless a license is suspended or revoked, or in the case of law enforcement issuing a citation, no record of identity verification is kept.

The second key component is that a phone never needs to leave the license-holder’s hand for a verification to occur. You present your phone for verification and you maintain possession the entire time. This not only ensures the privacy of the other personal information you carry on your mobile phone, it also eliminates the liability of a verifying party mishandling or possibly damaging your device.

To learn more about our DDL solution and our in-field experience, visit gemalto.com/ddlpilot