Governments and Digital Wallets

October 2023 | Version 1.1

Produced by:

Nick Mothershaw, with the input of the members of the
Open Identity Exchange Working Groups

CONTENTS

Please note that this document does not represent the views of Ofcom.

1 EXECUTIVE SUMMARY

Governments around the globe are tracking the evolution of digital wallets to try and determine how their citizens can use these to carry government issued credentials that enable a user to prove who they are and what they are eligible to do.

The EU for example is taking a pro-active approach to wallets: requiring all member states to issue their citizens with a EUDI Wallet that is certified to a common reference framework with the goal of achieving interoperability for access to government and private sector services across the EU.

Meanwhile, individual US states are issuing mobile driving licences (mDLs) into private sector smartphone wallets.

Governments, including EU member states, are asking the question:

- Who should provide the wallets?
- Should governments issue their citizens with wallets directly?
- Should wallets come from the providers of our smartphone operating systems as a captive wallet?
- Should relying parties issue wallets to meet their specific purposes, for example air travel or finance?
- Or should specialist regulated private sector wallet providers emerge, that will allow independent control and innovative features to attract users to their services?

This paper primarily explores the second question: Should governments issue wallets to their citizens?

In order to facilitate this exploration, OIX created 4 models of how governments might choose to interact with the world of digital wallets:

- Government provides a wallet to hold government issued credentials only
- Government provides a wallet to hold both government and private sector issued credentials.
- Government provides a wallet to hold government issued credentials and also allows approved private sector wallets to hold government issued credentials.
- Government does not provide a wallet but allows approved private sector wallets to hold government issued credentials.

In this paper we consider the pros and cons of each of these options. **The analysis leads us to conclude that option 4, where governments do not issue wallets but allows approved private sector wallets to hold government credentials is the preferred approach** because:

- Governments do not need to cover the expense of building and operating a wallet.
- Users have less fear that governments are monitoring their use of their wallet.
- Users can hold a mix of government and non-government credentials in their chosen private sector wallet(s), mirroring today's physical wallets that users are familiar with.

- Relying Parties can access, and users can provide, the mix of credentials required to fulfil a complex transaction, such as a government approved ID and a private sector payment mechanism, from the same wallet.

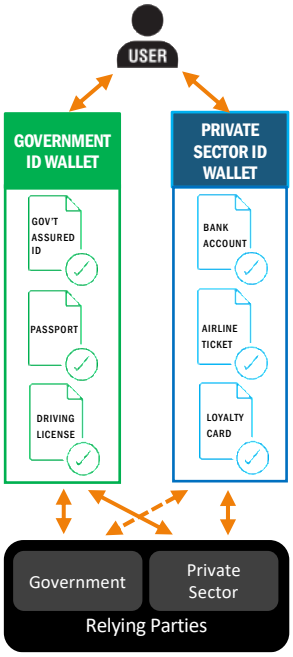
There are many more advantages to this approach for each of the above parties that are described in the following recommendations and conclusions section.

If the tech-giants want to hold and present government credentials in their wallets, they would need to be approved to do so by the relevant government that issues credentials for each market.

Canada has already recognised the need to manage wallets within the pan-Canadian Trust Framework and has issued a Wallet Conformance Profile. The EU is setting the conditions for member states to make a choice: state ID wallet provision, or provision of EUDI compatible wallets through private sector partners, whilst the UK is exploring how its' digital identity trust framework must evolve to support private sector wallets. So, governments are already on this route; we hope this paper informs the decisions of many governments in their approach to digital wallets, as they grapple with this fast-evolving opportunity.

2 MODELS OF GOVERNMENT-WALLET INTERACTION

2.1 Government provides a wallet to hold government issued credentials only



In this first model, government provides an ID wallet that contains government credentials. This will include some form of **'trust anchor'** credential, such as a digital version of a national ID or a recognized level of assurance. This contains core ID information about the user that has been verified by the government, or to a standard approved by the government: Name, Address, DoB, National ID number. The trust anchor is used to identify who the user is to allow them to store other trusted credentials in the wallet, removing the need for each issuer to re-identify the user who is asking them for a credential.

In the EU's eIDAS2 EUDI framework this trust anchor is the "PID" (Personal Identity Data) that must be issued by a member state and without which (type 1) EUDI wallets are inoperative.

In other country identity assurance approaches, the trust anchor might be a level of assurance determined to a government policy.

In this model, the Government ID wallet cannot be used to hold private sector credentials. Equally, private sector wallets are not allowed to hold government issued ID credentials.

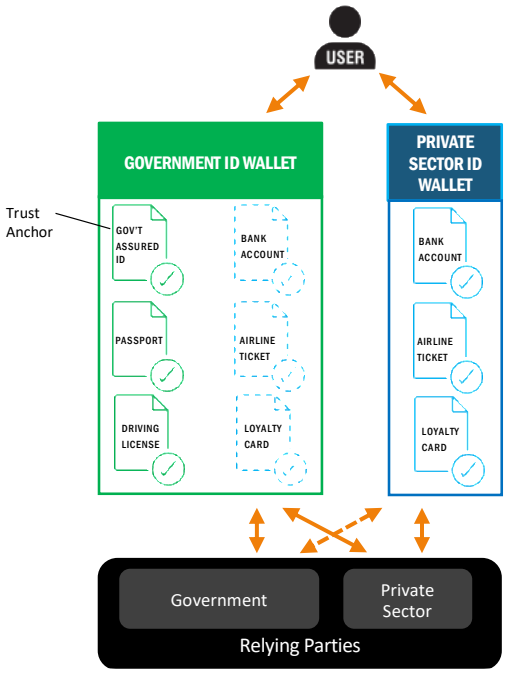
The Government ID wallet might be used to provide ID verification to the private sector. Equally government may accept non-government issued credentials from a private sector wallet for specific use cases. Users may have concerns that government might track their use of the government issued wallet in private sector use cases.

The challenge with this model is that the user will have private sector wallets too. They probably already have these on their smartphone as a built-in offering from their operating system provider (e.g., Apple. Google). So, the user will have at least 2 wallets. This contradicts a user's mental model of a wallet today, which is of a single physical wallet that contains a mix of government and private sector credentials e.g., driving license alongside a bank card.

In order to gather the credentials required to fulfill a specific transaction a relying party may need to access credentials from both the government wallet and a private sector wallet, requiring complex user interactions and costly integration costs.

Party	Pros	Cons
Government	Control of government credentials in a government issued wallet	Cost of build and management of government ID wallets
User	Trust in government issued wallet	Concerns government might track their use of the government provided wallet in private sector use cases. Multiple Wallets Complex interactions with Relying Parties
Relying Party	Trusted credentials from government wallets	Complex interactions with multiple wallets Poor user experience

2.2 Government provides a wallet to hold both government private sector issued credentials



In this second model, government provides an ID wallet that contains government credentials, including a trust anchor as explained above.

This Government ID wallet can also be used to hold private sector credentials. However, private sector wallets are not allowed to hold government issued ID credentials.

The Government ID Wallet might be used to provide ID verification to the private sector, including using private sector credentials already held in the wallet. Equally government may choose to accept non-government issued credentials from a private sector wallet for specific use cases.

The challenges with this model are:

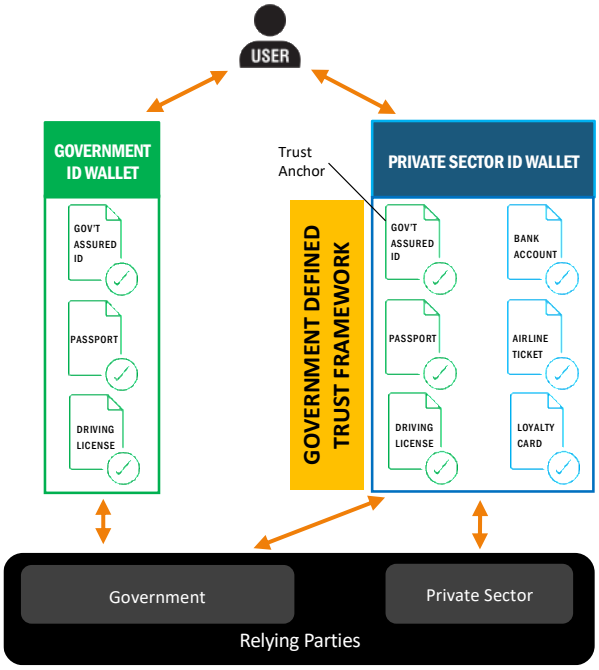
a) if the government wallet does not allow the user to hold all their private sector credentials, the user will be forced to have a private sector wallet too.

b) due to privacy concerns users may be uncomfortable in holding some private sector credentials in a government wallet, regardless of any assurances the government might give. Examples might include banking details, travel details or account access details that the user believes are none of the governments business.

c) governments will have to host and manage credentials issued by non-government parties, making operation of the wallet more expensive and complex from a security perspective. Logically and economically governments will only support some key common use private sector credentials, as supporting all credential types that exist in the private sector will be a never-ending task for no reward to the government (unless it charges for holding them).

Party	Pros	Cons
Government	Control of government credentials in a government issued wallet	Increased cost of build and management of government ID wallets User perception of government access to private sector credentials Increased complexity of security measures required
User	Trust in government issued wallet May be able to leverage one government issued wallet for many transactions.	Likely to still need multiple Wallets Complex interactions with Relying Parties Users may have concerns that government might track their use of the government provided wallet in private sector use cases. Reluctance to place private sector credentials in a government issued wallet.
Relying Party	Trust credentials from government wallets. May be able to leverage one government issued wallet for many transactions.	Residual complex interactions with multiple wallets for credentials not supported by the government wallet, resulting in poor user experience. Increased cost of maintaining multiple complex integrations

2.3 Government provides a wallet to hold government issued credentials and also allows approved private sector wallets to hold government issued credentials.



The third model involves a government provided ID wallet that contains government credentials but one that does not hold private sector credentials. This can then be used in the context where only government credentials are required, or perhaps where a government wallet is the only way to access government services only; the UK One Login model could be loosely argued to follow this model.

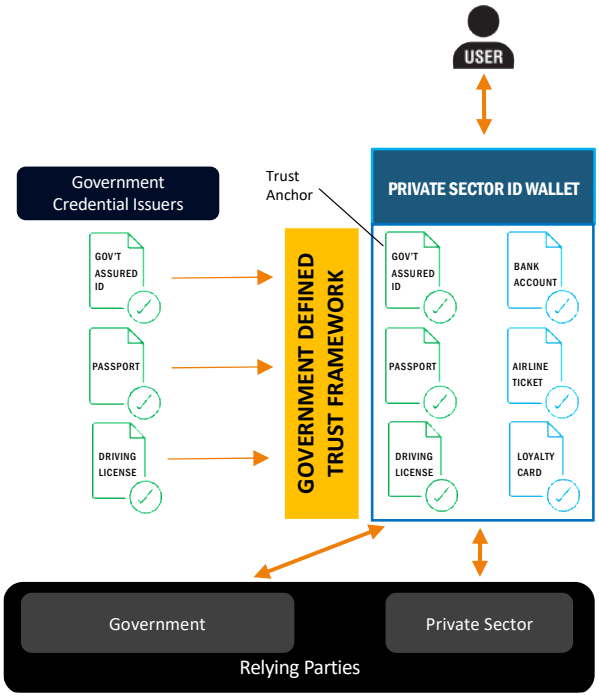
In this model the government also allows government credentials, including a government issued 'trust anchor' to be held in approved private sector wallets. Approval of private sector wallets could be via their certification to a government defined trust Digital Identity Trust Framework.

The user can then collect government and private sector credentials in a trusted private sector provided wallet, removing the fear that government might have access to credential use. This also has the advantage that the private sector wallet provider can ensure that the government and private sector credentials that are needed to meet complex multi-credential relying party use cases are available as commercial and competitive feature of their wallets. The user may have the option to use one private sector wallet for most of their transactions if they choose to.

Party	Pros	Cons
Government	Control of government credentials in private sector wallets through approval of which wallets can hold them No user perception of government access to private sector credentials Control of the data (ID) and the way it is handled rather than the devices doing the handling.	Cost of build and management of government ID wallet Loss of sole control of government credentials in a government issued wallet
User	Trust in government approved private sector wallet Users may have less concerns that government might track their use of the government issued credentials in private sector use cases. May be able to leverage one private sector issued wallet for many transactions. Less likely to need multiple Wallets	May still need a government wallet if one is required to access government services.
Relying Party	Trust credentials from government approved wallets. Should be able to leverage one private sector issued wallet to access all credentials.	Charges from private sector wallets for access to government credentials, unless this is underwritten by government*

*OIX will be producing a separate paper on commercial models for wallets for release in early 2024.

2.4 Government does not provide a wallet but allows approved private sector wallets to hold government issued credentials.



In this final simpler model, government does not provide its own ID Wallet.

Government allows government credentials, including a government issued 'trust anchor' to be held in approved private sector wallets, such as a digital version of a national ID or a trust framework recognized level of assurance. Approval of private sector wallets could be via their certification to a government defined trust Digital Identity Trust Framework.

Access to government services would be via an approved private sector wallet.

The user can then collect government and private sector credentials in a trusted private sector wallet, completely removing the fear that government may have access to credential use. Private sector wallet providers can ensure the government and private sector credentials that are needed to meet complex multi-credential relying party use cases are available as commercial and competitive feature of their wallets. The user may have to the option to use one private sector wallet for most of their transactions if they choose to.

Party	Pros	Cons
Government	Control of government credentials in private sector wallets through approval of which wallets can hold them Control of the data (ID) and the way it is handled rather than the devices doing the handling. No user perception of government access to private sector credentials No cost for build and management of government ID wallet.	Loss of direct control of government credentials in a government issued ID wallet
User	Trust in government approved private sector wallets. Will be able to leverage one private sector issued wallet for many transactions. Users may have less concerns that government might track their use of the government issued credentials in private sector use cases. No need for multiple Wallets Best user experience across all use cases	
Relying Party	Trust credentials from government approved wallets. Will be able to leverage one private sector issued wallet to access all credentials.	Charges from private sector wallets for access to government credentials, unless this is underwritten by government*

*OIX will be producing a separate paper on commercial models for wallets for release in early 2024.

3 RECOMMENDATION AND CONCLUSION

The recommendation of this paper is that governments do not provide their own ID wallets to citizens.

Governments should create trust frameworks to enable the approval and trust of private sector provided wallets, and then issue government credentials only into approved private sector wallets.

This approach has the following advantages for governments:

- Cost Savings: No need to develop, maintain, secure, provision, integrate and manage a government issued ID wallet.
- Focus by the government on the security of the government issued credential containing the identity data, will enable the private sector providers to focus on the wallets, devices and applications that are required to handle that data securely and cost effectively
- Can move to a more decentralized approach to identity management where private sector providers are required to implement decentralized user-centric data management.
- Time to market. Digital ecosystem can be more quickly enabled by leveraging private sector wallets and speed to market.
- Allows for innovation in Digital ID services through competitive private sector wallets.
- Government can focus on issuing government credentials to approved wallets.
- Private sector is better suited to evolving digital ID to meet different delivery modes (e.g., not on a smartphone, cloud wallets). Means a more inclusive approach as a smartphone is not a pre-requisite for an ID wallet.
- Creates a private sector market for wallets, enabling economic growth, rather than a taxpayer funded ID utility.
- Accessibility and Delegated Authority can be achieved by specialist private sector providers.
- Mitigates the risk of government delivered ID wallets suffering from technology and innovation stagnation
- Private sector wallets can link users to the legal entities they represent, removing the need for government wallets to tacking his complex issue, and removing transparency to government of personal to LEI relationships.
- Private sector wallets can work across government boundaries, enabling access to services for non-national subjects in a seamless way, enabling further economic growth.

The private sector wallet approach has the following additional advantages for end users:

- Users could choose to manage all their credentials in one wallet, enabling seamless access to multi-credential transactions. Equally users could choose to have several digital wallets for different aspects of their life. For example, we do this today, as we may have a different wallet when we travel, with a separate section for business purposes. Users will choose a private sector brand they trust to manage their wallet for them. The government trust framework enables this trust.
- Users are likely to have fewer concerns that government might track their use of the government issued credentials in private sector use cases.
- There is an argument that no single wallet solution will meet all use cases as the possible credential needs are too broad. This approach allows the user to hold several specialist government approved wallets for specific purposes e.g., Travel, Health, Education that can each carry the relevant government issued credentials.
- Users, privacy campaigners and the media do not perceive government has a master ID database through provision of a government provided wallet. Nor do they perceive the government can track what they are doing through a government provided ID wallet.

In addition, relying parties will also benefit from this approach as:

- They should be able to access all the credentials they need to meet multi credential transactions through interfacing with one wallet that specialises in their complex requirements, resulting in cheaper costs for credentials and integration.
- Smart wallets could process complex rules for multi-credential questions (e.g., to travel to XYZ you need a passport and a covid test), pushing complex processing to a third party.
- They may be able to assign some liability for incorrect or fraudulent data to the private sector ID provider. It's unlikely that governments will offer any such liability cover.
- Time to market should be improved with access to credentials quicker. More users with Digital ID wallets, more quickly
- Security resilience through continued innovation, rather than security of oldest supported version that tends to prevail in government systems thinking.
- Relying parties have commercial choice and leverage, which will keep the market price for credentials competitive. Weaker wallet players will be corrected or rejected by market forces.

Finally, any perceived loss of control or oversight by the government can be addressed by:

- Ensuring the trust framework for wallets provides standards to ensure good quality credentials management and use.
- Building oversight into the trust framework to which private sector wallet providers must be certified.
- Ensuring the ability to move credentials from one wallet to another through portability requirements.

- Build into the trust framework control over which entities can use a government credential, without the government knowing when or where the credential is used.
- Build into the trust framework an ability for the government to withdraw its credentials from wallets that fail to maintain the required standards.

Some governments may choose to issue their own ID wallets under the framework so that citizens have a non-private sector choice of wallet available in the market (per option 2.3). Whilst giving users an alternative may be a good idea, it will mean the government will need to deal with the costs and evolution implications of issuing and manage their own wallet.

So, with significant advantages and mitigable control concerns, it can be concluded that enabling approved private sector wallets under a government approved framework (or scheme), is the best approach for governments, their citizens and relying parties alike.