

e-Society and e-Economy Enterprise Architecture

High level overview

August 2023 v1.2

Table of contents

Introduction	2
Vision for Armenia's e-Society: Data as a National Wealth	2
Core Principles of the architecture	2
1. Public agencies retain their mandate for service delivery	3
2. E-society architecture must enable cooperation	3
3. E-society architecture must have a clear legal and policy foundation	3
4. Proactive portfolio management and appropriate governance	3
E-society architecture description	4
Conceptual overview	4
Detailed description of the layers	5
Conclusion.	8

Introduction

In the digital age, countries around the world are redefining service delivery models by harnessing the power of technology and data. Armenia is embarking on a transformation journey towards an e-Society and e-Economy. At the heart of this vision lies the recognition that data is a national wealth, serving as the bedrock for personalized, convenient, and user-centered digital services. This paper is intended to outline the Armenian Government service architecture, highlighting core principles and components, each component will be elaborated further in future editions.

Vision for Armenia's e-Society and e-Economy: Data as a National Wealth

Armenia aspires to become an e-Society and e-Economy (e-Society), where the seamless integration of technology and data empowers its citizens, businesses and public agencies alike. By treating data as a national wealth, Armenia will change the way government services are designed, delivered, and experienced by end users.. This vision places the individual citizen and business at the center, a future where digital interactions are intuitive, personalized, and tailored to the needs and preferences of citizens and businesses. The transformation will be inclusive, providing accessible services to all parts of society.

Core Principles of the architecture

The e-Society service architecture is designed with 3 key principles in mind, these principles ensure that the development of the e-society vision is sustainable, in-line with Armenia's democratic governance and does not slow down innovation.

1. Public agencies retain their mandate for service delivery

Public agencies form the central part of the architecture. They are free to provide services based on their constitutional, democratic mandate and availability of resources. In practice, this means that they can innovate at a pace which is suitable for them.

2. e-Society architecture must enable cooperation

While comprised of independent branches, the government should act as a unit. Therefore, the e-society architecture supposes that individual agencies are linked by layers of cooperation. Each provides technical and organizational means for agencies to jointly solve the complex problem of offering low-friction services in a holistic manner. To aid cooperation with the private sector, all layers can be extended to include private sector. The layers each consist of technical infrastructure surrounded by a community of stakeholders enabling technical collaboration, overseen by the state bodies defined by law. In addition, each layer should have a corresponding strategic collaboration community run by and focusing on higher-level issues. The layers can also be operated by the private sector through Private-Public-Partnership (PPP) agreements.

3. e-Society architecture must have a clear legal and policy foundation

Armenia has circulated and will adopt 4 key legal acts in order to enable the full implementation of the e-society architecture. The renewed laws on Population Register (the core register for master data on the population) and on Digital Identity and Trust Services. The new laws on Cybersecurity, and on Public Information. The adoption of these key laws will act as the foundation for Armenia's transition to an e-society, setting the parameters & legal frameworks from which the technical solutions will be deployed.

4. Proactive portfolio management and appropriate governance

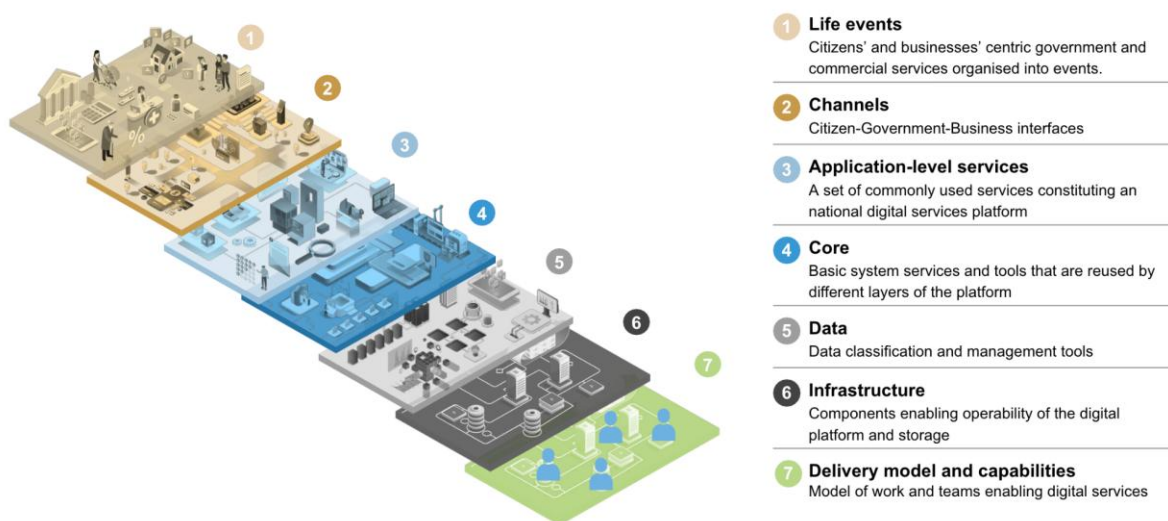
The legal acts and policies are linked to the architecture by the finance and portfolio management processes, that fund development of and integration with the architectural components, and direct agencies to develop solutions fitting with the architecture and reduce duplication of effort by favoring joint investments and decisions based on 'business cases' over development of siloed technical 'systems'. This governance is

managed by the Information Systems Management board, with cross governmental representation, chaired by the Chief Information Officer of Armenia. (Currently this role is assumed by the Deputy Prime Minister).

e-Society architecture description

Conceptual overview

Figure 1: Summary description of the e-Society architecture layers

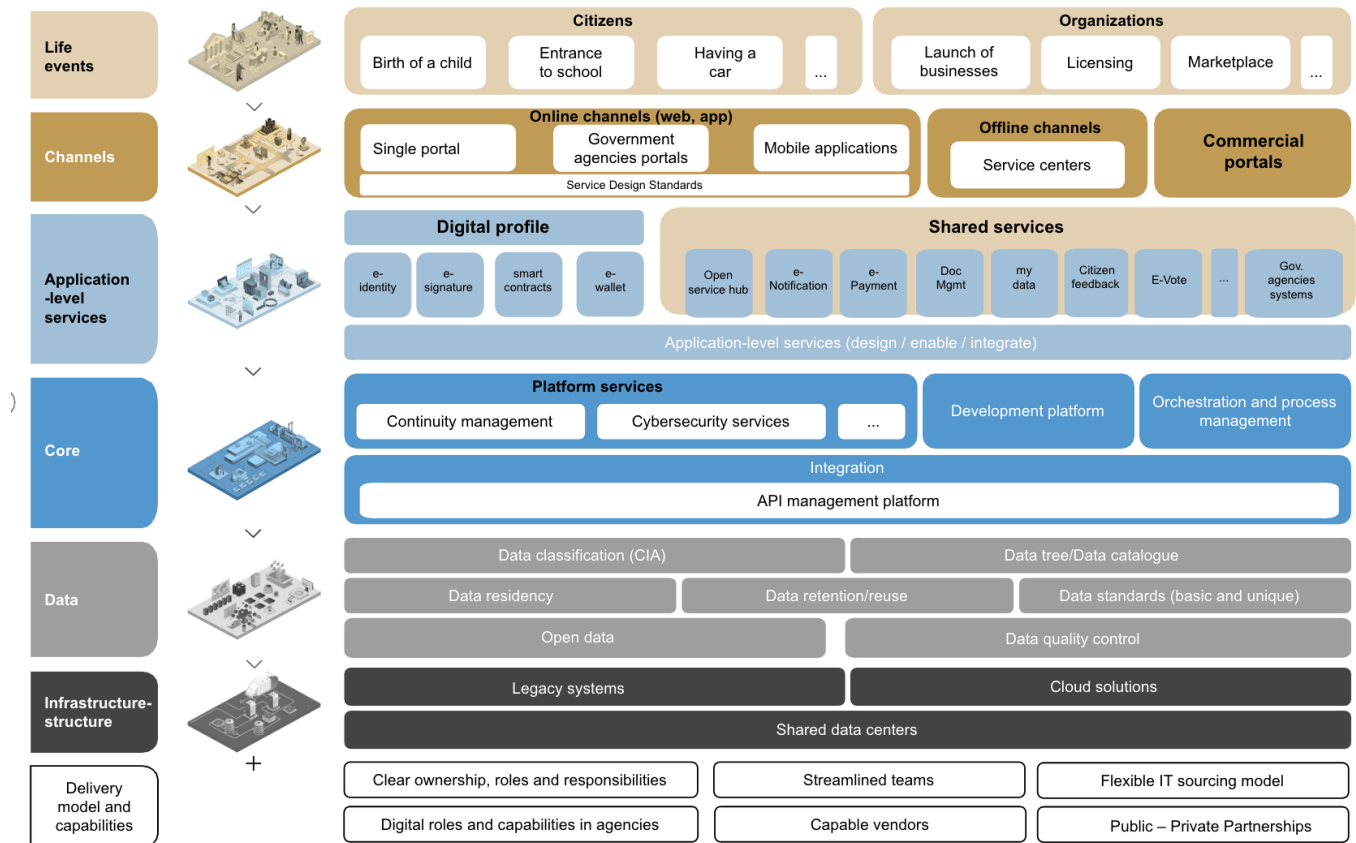


The 7 layers of the e-Society service architecture are intended to provide a framework for cooperation between state bodies & the private sector, all brought together through the concept of life events.

The advancement of the e-Society architecture relies on proactive engagement between state, private sector, and civil society actors. This collaborative approach leverages the strengths of each sector to create a comprehensive, innovative, and user-centered digital ecosystem. Through these interactions, the e-Society architecture becomes a dynamic and responsive framework that will address the ongoing societal needs while upholding principles of inclusivity, transparency, and efficiency.

Detailed description of the layers

Figure 2: Layer diagram



Life events

This is the key interaction point between citizen and public bodies. The life event approach in an architectural context can be considered to be the grouping of various services provided by state bodies, together with clear, concise information informing users about their legal rights, access to state assistance and their legal responsibilities. For example, the 'starting a business' life event could include information and guidance on types of business activity permitted, with integrated links to register a business, information on tax regimes, and the creation of a tax account, through to provision of accounting services. All state bodies will be delivering their services through the prism of a life event. This will require inter-agency collaboration and will be enabled by the other layers of the e-society architecture.

Channels

During the life event, service delivery will be conducted through an omnichannel approach. The state agencies are free to consider the most optimal delivery channel for services - finally, all provided services will be collated onto a single portal. The successful enablement of interoperability will also allow for an increase in 'automated' service provision or 'zero channel' delivery, for example, upon the birth of a child, a user may be provided with access to state benefit, simply by providing consent, rather than completion of an application form. Ministries and state bodies will be encouraged, through the e-Society architecture, to consider the optimum delivery channel based on a number of key factors, including technology, organisational/management burden and user experience.

Despite the associated costs, a mix of delivery channels is common for service delivery. Creating that mix depends heavily on the strategic context of the service, but the guiding goal should always be to provide the most suitable user experience while adding the lowest amount of cost and complexity to the organization and its information system.

Mobile first considerations:

The mobile application as a delivery channel has capacities not easily available on other channels like direct interaction via notifications, integration with other apps and capabilities of mobile devices, content creation etc. Despite this, , delivering services via mobile apps also involves significant downsides, mainly the need to support a multitude of operating systems and (limited) screen sizes and the inability to change the user experience at will. Also, mobile applications are typically not stand-alone entities and require server-based infrastructure to a similar extent a web application would. Finally, downloading a mobile app presents the user with an additional commitment they are not necessarily willing to make. These downsides mean a mobile app tends to be useful in scenarios, where the fluidity of the user experience outweighs its downsides due to, for example, the sheer number of interactions. Many necessary interactions can be, however, a sign of bad service design or indicate an opportunity for use of the non-channel.

Upsides

- Unique capabilities not available via other channels
- Good for regular use scenarios e.g. situations where you regularly need to do the same thing numerous times.
- Potential for seamless user experience difficult to match via other channels
- Device presence can offer some security features not available elsewhere
- Low variable cost
- Scales well up to a relatively high transaction volume

Downsides

- Lack of flexibility in terms of pushing changes to the user experience

- Need to maintain a similar user experience across multiple operating systems, screen sizes and modalities
- More sophisticated user interaction (e.g., collecting information from multiple sources, making precise adjustments, presenting large amounts of complex information etc.) can be challenging
- Significant barriers to responding to calls to action by the service providers (e.g., receiving a notification of license expiry without having the appropriate app downloaded)
- Significant capex and moderate to high opex

When to use

- For frequently used services with no fixed schedule (e.g., bank transfers, hunting/fishing permits)
- For services requiring two-way interaction with the user (e.g., filing insurance claims with photos of the incident and receiving notifications on the progress of the claim)

Therefore, state agencies will firstly be recommended to consider delivery channels required by regulation or nature of the services and then consider the implications of adding additional channels. For example, if a service process must, by law, terminate with a physically signed document or the organization is required to maintain a regional presence in the country, a physical service channel is a necessity and developing web or mobile channels would add cost and complexity without much additional benefit. (unless, elimination of the physical necessity can be eliminated via legislation).

Finally, if a service can be fully automated, a zero-channel should be the first choice with additional channels only utilized for fringe cases as required. In short, the following approach will be recommended:

1. Determine the minimal physical channel presence necessary and allocate services to it.
2. For the reminder of services, establish a path towards a zero-channel where possible.
3. For the reminder of services, determine if a mobile app provides material advantages over the web channel.
4. Develop a mobile-ready web channel for the reminder of services.

A further elaboration of the channel strategy will be published in the near future.

Government service portal: This is a lightweight, mobile responsive web portal that will be the 'starting point' for interactions during a life event. Mobile first, in this context means that the service is responsive and fully functioning on a mobile. From this portal, the users will be directed to the various 'service hubs' of each ministry and private sector services. In order to ensure consistency between services, a set of service design

standards is provided to ensure a common user experience across public service delivery channels, as well as mandatory measures for user satisfaction, to be published on the open data platform. The single portal will also provide access to the 'My data' panel - a consolidated view of all data held by the various government and private sector bodies, enabled by interoperability.

Application level services

These are shared services that will be provided as part of the e-society. They can be considered as 'enablers' for service provision and are designed to provide public agencies with a fast and efficient way to deploy services that are secure and easy to use.

Key components of this include a suite of 'digital profile' services:

e-Identity/signature portal: a central identity infrastructure which will provide a secure way for service providers to authenticate users. This will provide a single 'gateway' for users to sign-in to digital services (both government services, and private sector). the infrastructure will be provided as code, along with an onboarding and offboarding model, and standard API endpoints for integration

The architecture also includes a suite of shared application services: e.g. open service hub: this is a low/no code platform which will allow ministries to build simple services using a no code interface, multiple instances of these service hubs can be deployed to ensure de-centralisation and reduce risk, such as a shared service hub for social services. It is important to note that whilst the application services are provided to public agencies, their creation or operation will be done in collaboration with the private sector. As such, where it is deemed that the private sector can better provide a particular application level shared service, then this shall be considered a preferred approach - with the government ensuring appropriate oversight and regulation.

Core

These include elements that are integral to all services, regardless of the chosen service delivery approach or channel. Highlights include: Cybersecurity services, the provision of a central Security Incident Response Team (CSIRT), and a Computer Emergency Response Team (CERT) to ensure that services can be provided with the appropriate security monitoring, in addition to the required capabilities to monitor at the public agency level. Another key component is the 'Interoperability platform', this will be the shared technology protocol to allow secure data exchange between state bodies to provide services - this protocol and platform will allow for the implementation of the 'only once' principle (whereby a user should not have to provide the same information to more than one state body). The interoperability layer will also be opened to the private sector, to ensure wide adoption and enable the e-society architecture outside of the boundaries of public service delivery.

Data

The concept that data is a national wealth is core to the architecture. If data is to be regarded as a national wealth, then the appropriate controls, classifications, management methods and standards must be in place to protect it. Supported by the legal provisions in the future "Law on Public Data", public agencies will be required to carry out data mapping and classification on their registers, before being granted access to the interoperability platform. This will ensure that all data is eventually brought to a level that it is basic and unique. Where appropriate, public agencies will publish data to the national open data platform. In addition, data classification and management policies will be designed to be 'cloud ready' - to enable a smooth transition to the appropriate infrastructure. Wherever possible, international best practice and standards will be adopted. For end users, the 'my data' shared application will provide an overview of the data held about the, ensuring control and retention of the right to privacy.

Infrastructure

The e-society architecture calls for a multi faceted approach to infrastructure design and implementation. Subject to the required data mapping and appropriate classification, it is planned to enable public agencies to have access to shared cloud infrastructure through either the appropriate framework agreements with cloud providers, or a centralised procurement, in either case the goal is to enable simplified procurement and faster service delivery. Where deemed necessary, a hybrid cloud approach will be adopted, again, with an emphasis on standardisation and close cooperation with the private sector. The final approach to public digital infrastructure will be published in further elaborations of the e-Society architecture - but the current legacy of individual mini 'server rooms' at each public agency will be avoided.

Delivery model and capabilities

It is clear that in order to enable the e-Society architecture, public agencies must develop the necessary capabilities to make clear, concise business cases for the creation of digital services, design them in a way that is user centric, and ensure their continued management and secure maintenance. The e-Society architecture calls for a number of solutions to this problem: We intend to strengthen the capabilities in public sector agencies through carrying out multiple 'interventions' at various levels. Interventions include the implementation of pilot projects on life events, where public agency teams are provided with 'shadowing' resources to address key capability gaps, (for example: service management, technical architecture). Other interventions include embedding key digital capability directly into the state agencies, for example, through secondments from the private sector and experienced international professionals. The ultimate goal is to ensure that the public agencies have enough digital capability to act as well informed designers, purchasers, and operators of e-Society services (either through in-house capability or partnerships). Another core intervention for capability development is the implementation of key standards in information security and cybersecurity. This intervention covers both the private and public sector, where

cybersecurity skills are lacking overall. The e-society architecture calls for a nationwide capability 'uplift' through education, training and guidance on adopting key international standards in cybersecurity. A further elaboration on addressing capability gaps will be published in the near future

Conclusion.

The e-Society Service Architecture outlined in this document represents a comprehensive approach to transforming Armenia's governance and service delivery models in the digital age. By treating data as a national wealth and centering the architecture around personalized, user-centered digital services.

The core principles that underpin this architecture—public agencies retaining control over service delivery, enabling cooperation, and establishing clear legal and policy foundations—reflect Armenia's commitment to democratic governance, innovation, and sustainability. This forward-thinking approach ensures that the architecture is adaptable, responsive, and in harmony with the evolving needs of society.

At the heart of the architecture's design is the concept of life events, which acts as a pivotal point of interaction between citizens and the state. This approach streamlines service delivery, encourages inter-agency collaboration, and places the user experience at the forefront. The establishment of various layers, from channels to infrastructure, further enhances cooperation between state bodies, the private sector, and civil society, resulting in a dynamic and resilient digital ecosystem.

Critical to the success of the e-Society architecture is the proactive engagement between stakeholders, including the state, private sector, and civil society. This collaborative endeavor leverages the strengths of each sector, ensuring that the architecture evolves in a way that is inclusive, transparent, and efficient. By fostering this synergistic relationship, Armenia sets the stage for a transformative journey towards an e-Society that not only embraces technological advancements but also upholds fundamental principles of governance, security, and user-centricity.

As Armenia embarks on this path, further iterations and elaborations of the e-Society architecture will undoubtedly refine and expand its components. The e-society architecture will act as the driving force to redefine the relationship between citizens and their government, ushering in an era of digital empowerment, accessibility and holistic service delivery.

Review history:

Name	Org	Version
Arman Khachaturyan Arman.Khachaturyan@isaa.am	ISAA	1.2
Nerses Yeritsyan nerses.yeritsyan@cba.am	ISAA	1.1
Harmick Azarian harmick.azarian@isaa.am	ISAA	1.0