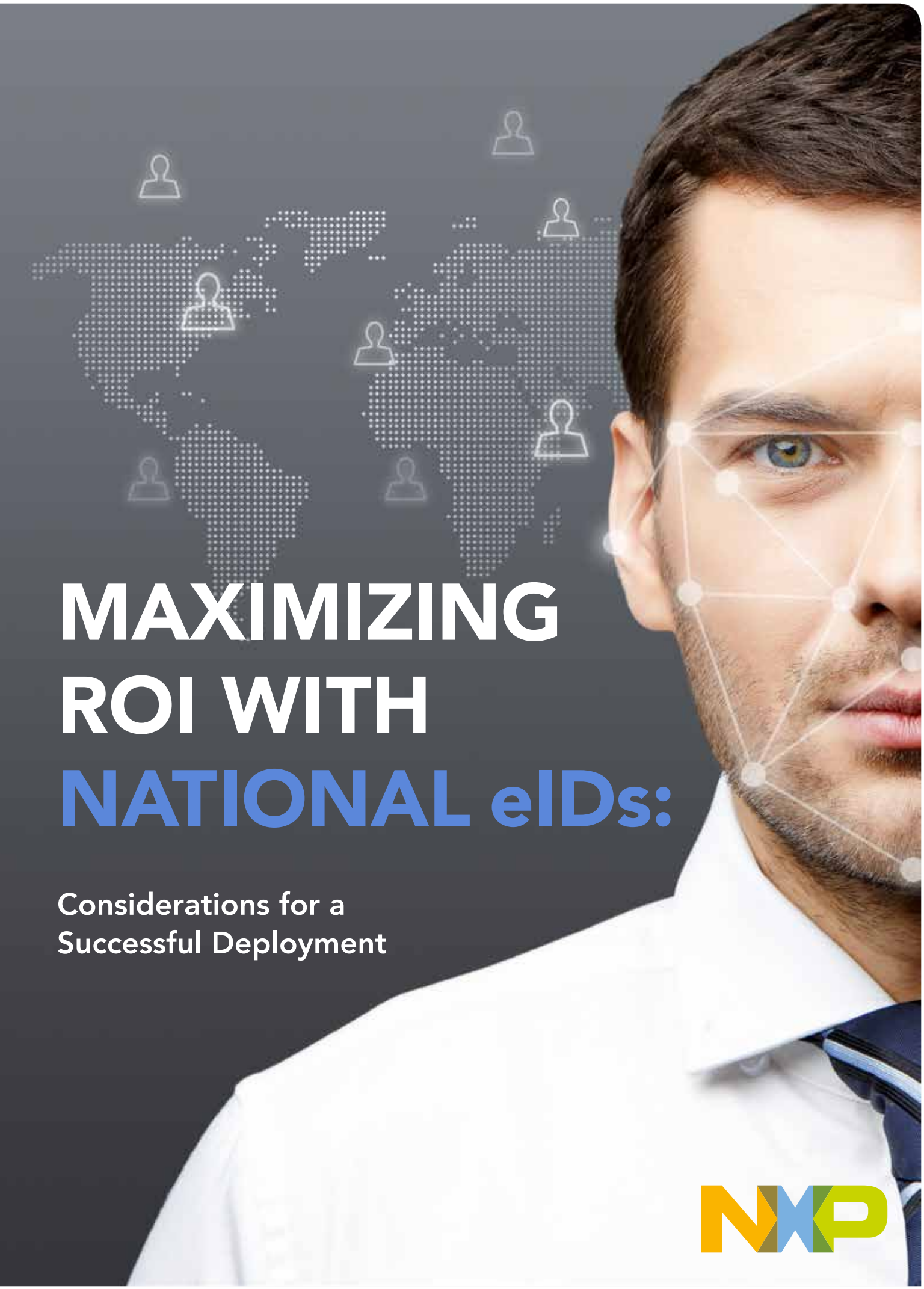
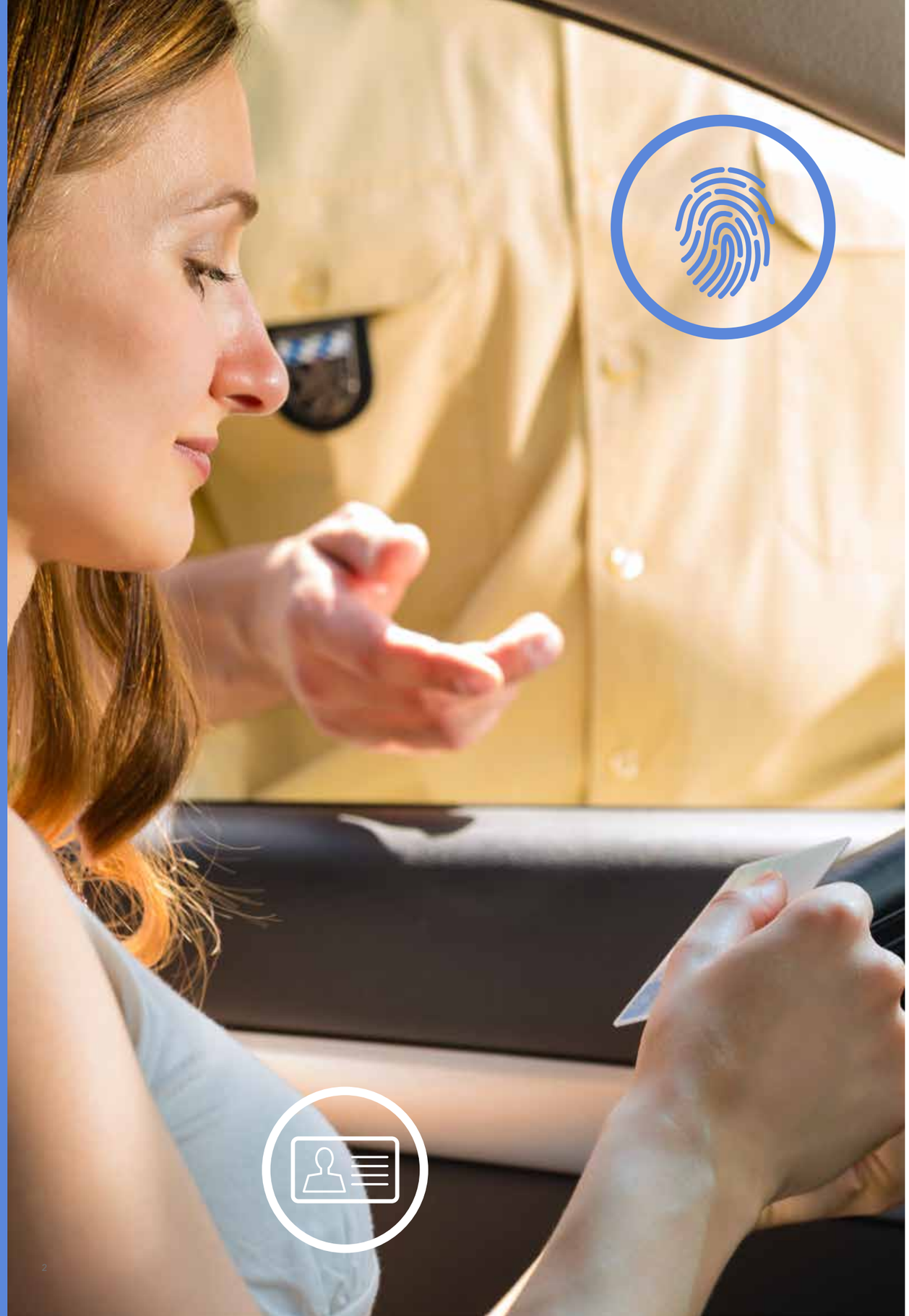


MAXIMIZING ROI WITH NATIONAL eIDs:

Considerations for a Successful Deployment



Developing and implementing a national program for **electronic IDs** (eIDs) is a complex, time-consuming, and expensive undertaking. Each country does things a little differently, but we've found that there are several things that all successful eID deployments have in common. This paper looks at best practices, so national governments can ensure security and convenience while reducing costs, working more effectively, and maximizing their return on investment.

CONTENTS

WHY GO FOR AN ELECTRONIC ID?

There are now dozens of countries worldwide that have upgraded their national identity programs to support **electronic IDs**, and more are on the way. The research company Acuity Market Intelligence predicts that, by 2018, there will be more countries issuing eIDs than those issuing traditional, non-electronic IDs, and there will be at least 3.5 billion eIDs in circulation globally.

Why are so many national governments transitioning to eIDs? Because making the move from analog to digital delivers several benefits, especially in terms of data security, cost savings, and citizen engagement.

GREATER CITIZEN SATISFACTION

Digital IDs make it easier for people to access government services and enjoy the benefits of citizenship, and that helps increase citizen satisfaction and engagement. Faster transaction times mean less waiting, with shorter lines in government offices. Having digital credentials makes it easier and safer to use online services, so there's less need to go somewhere in person. A nationwide eID can increase opportunities for democratic participation, with more transparent voting processes, and can enable financial inclusion, by supporting cashless transactions. Also, when eIDs are linked to additional services, including those provided by private-sector organizations, a single credential can be used with a wide array of day-to-day activities, from public transport and payments to physical and logical access.

INCREASED SECURITY

The eID format, which uses microprocessor-based smartcard technology to store and protect personal information, makes citizen data more secure, and as a result helps combat identity theft and reduce fraud. That, in turn, makes government programs more effective and more efficient, and lowers the cost of providing services. Increased security can be of particular benefit to a number of government-funded activities, such as healthcare services, social-welfare programs, and tax collection, which are often targeted by scammers.

LOWER TRANSACTION COSTS

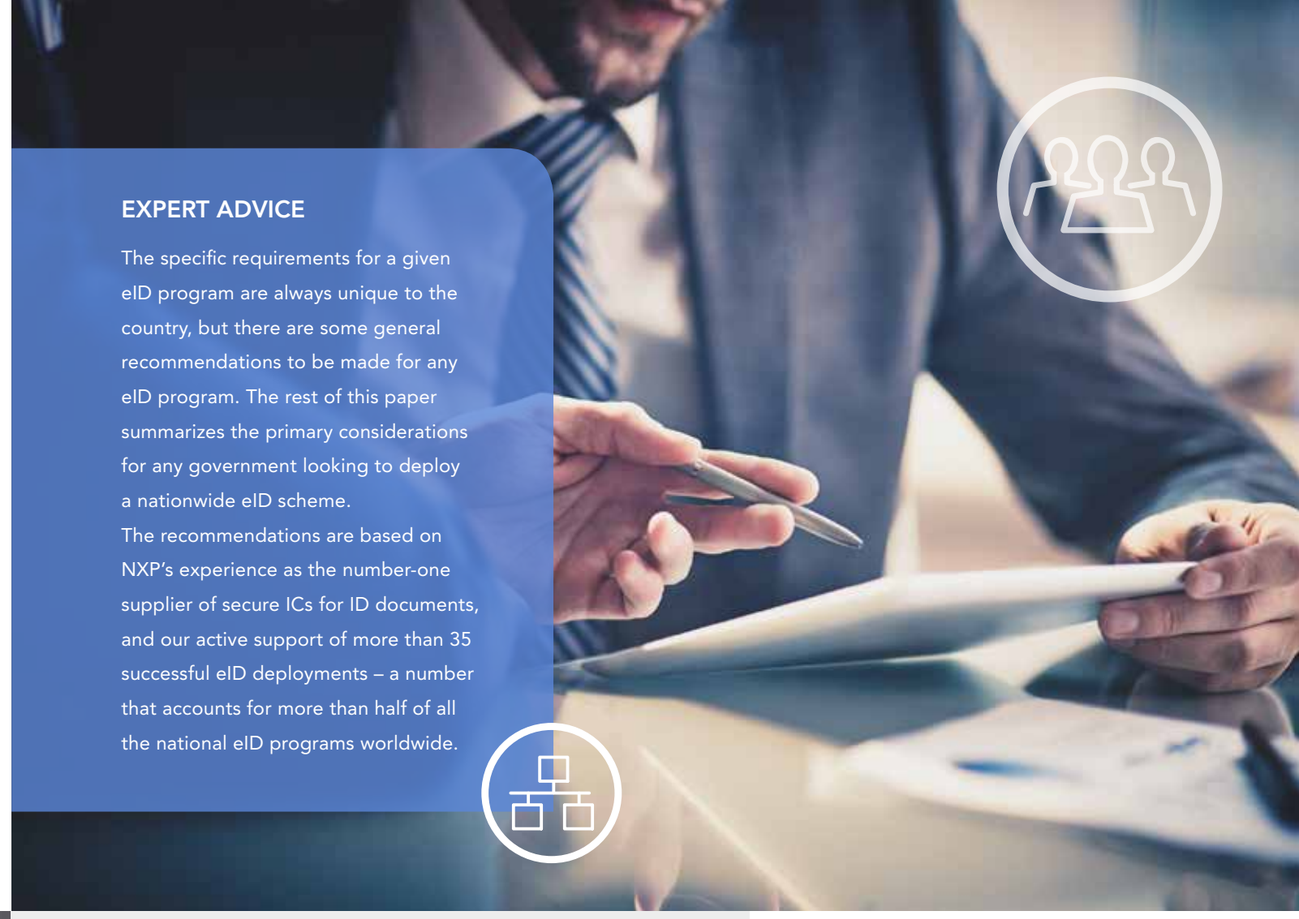
Because eIDs are read and authenticated by dedicated readers, they increase automation and lower the cost of each transaction. With traditional, paper-based IDs, the transaction costs are mostly associated with the labor required to process the request. With digital IDs, the use of electronic readers reduces transaction times and enables automated self-service, which in turn lowers service-center cost.

All three of these benefits – data security, transaction costs, citizen satisfaction – combine to create significant savings, in the form of lower operating costs. The prospect of increased effectiveness, long-term savings, and a positive return on investment, may well justify launching an eID program, but there's another reason to consider eIDs, too. For many, including the United Nations, eIDs are a building block for the future.

FOUNDATIONAL TECHNOLOGY

Building an infrastructure that supports the use of eIDs and digital signatures is an essential part of the Whole of Government (WoG) approach to service delivery, which aims to make public administration more sustainable. As defined by the United Nations in their 2016 report on eGovernment, WoG service delivery refers to services from various public agencies bundled together and accessible from one point of entry. The WoG approach, which relies heavily on eGovernment technology, including eIDs, makes it simpler to interact with public administration and, at the same time, helps public service agencies work together "across organizational boundaries in a shared response to particular issues."

The WoG approach, with its emphasis on integrated services, is gaining momentum. According to the 2016 UN Survey, "90 countries (including over 50 developing countries) provide a link to a one-stop-shop service platform; 105 countries provide advanced search features; 98 countries require digital ID for online or mobile services, and 71 countries provide an online tracking system." Making eIDs part of the login process for any of these integrated services helps increase security and protect citizen data.



EXPERT ADVICE

The specific requirements for a given eID program are always unique to the country, but there are some general recommendations to be made for any eID program. The rest of this paper summarizes the primary considerations for any government looking to deploy a nationwide eID scheme.
The recommendations are based on NXP's experience as the number-one supplier of secure ICs for ID documents, and our active support of more than 35 successful eID deployments – a number that accounts for more than half of all the national eID programs worldwide.

ENSURING RETURN ON INVESTMENT (ROI)

National governments thinking about launching an eID program, as a standalone initiative or as part of a broader eGovernment strategy, have a lot to consider. Planning, developing, and operating a nationwide eID program is a large-scale, long-term undertaking.

The choices made during the initial planning process can influence the level of complexity, the time it takes to implement the plan, the overall cost of the rollout, and the longer-term return on investment. For an efficient rollout and maximum ROI, it's important to leverage industry expertise, so as to build on best practices for deploying a successful eID program.

WHERE TO START: VISION, LEGAL MANDATE, TECHNOLOGY

Nationwide eID programs are very visible projects. Creating a solid foundation for growth, while saving money throughout the implementation and fostering citizen support, success and increase ROI.

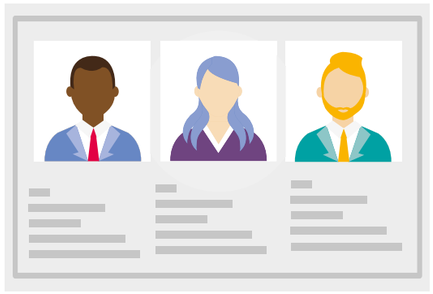
In our experience, there are three things needed to create a strong foundation for a nationwide eID program: a clear vision, a legal mandate, and a strong technical framework.

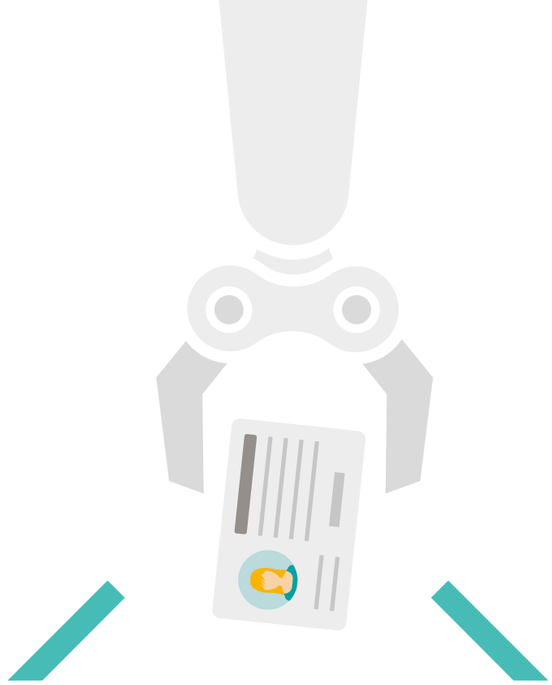
1. BE CLEAR ABOUT WHAT YOU'RE BUILDING

It's important to create the right program for your needs. Begin by defining the eGovernment strategy and derive the respective use cases and business models for the eID program accordingly. This part of the process can take a considerable amount of time and effort, since it means aligning with various public and private stakeholders. Communicate your vision to show that taxpayer money is being spent wisely, and that services in the public and private sectors are gaining efficiency.

2. MAKE IT MANDATORY

Clearly define the use cases that mandate the secure authentication of a citizen and establish the necessary legal framework to support those use cases. The legal framework ensures that any rules for the use of eIDs, especially with services requiring a high level of trust, such as opening a bank account, will be enforced.





3. IDENTIFY A BASELINE CONFIGURATION

Create a solid starting point by defining the technology framework and its baseline functionality. The baseline configuration provides a generic authentication token for all the current and planned services. It should, for example, support on and offline authentication, and should include enough memory to support the data required for existing and upcoming functionality. The baseline configuration provides a platform that can be expanded incrementally to support new applications, after the initial rollout or as part of a phased introduction. To ensure sufficient flexibility to support future use models, an open platform is strongly recommended.

The next section looks at more specific guidelines to consider for the baseline configuration, and the requirements that enable ongoing expansion and evolution of an eID program.

CREATE A FOUNDATION FOR GROWTH: THE BASELINE CONFIGURATION

As mentioned above, the **baseline configuration** should support all the use cases defined for the initial rollout, such as those required by law enforcement, border-control agencies, government agencies, private-sector services, and so on. The baseline configuration should also be both flexible and robust enough to support expansion over time, to support use cases that aren't yet available but will be soon.

GENERAL GUIDELINES

Aside from the standard eID use cases, there are a few other guidelines to consider, too. The items listed here can lower the total cost of ownership on the long run while ensuring security scalability and flexibility for future enhancements and programs extensions.

CONTACTLESS INTERFACE

The ISO 14443 interface enables contactless communication between the card and reader, for higher security and durability, lower maintenance costs, and greater ease of use. The chip and antenna are laminated inside the card and therefore protected against wear and tear, as well as tamper attempts. Compatibility with ISO 14443 (e.g. MIFARE) also creates options for multi-application use, as the eID can be made interoperable with other applications, such as transport ticketing, building access, micropayment, loyalty, and bike sharing.

JAVA CARD / GLOBAL PLATFORM OPERATING SYSTEM

An operating system compliant with Java Card GlobalPlatform allows maximum flexibility to add and drop applications, and makes it easier for government stakeholders to develop their own applets and create local content.

ICAO CONFORMANCE

There are several security mechanisms in accessing data stored on the card. For greatest interoperability with standard infrastructure equipment – and to save deployment time and cost – it's best to follow the guidelines already established for electronic passports, as defined by the ICAO specifications BAC, EAC, and SAC.

COMMON CRITERA SECURITY

To ensure and proof high secure technical solutions a Common Criteria Security Certification is a must. The product evaluation of a third party institute is necessary to assure customers that the products they are buying protect important assets against sophisticated attacks.

PUBLIC KEY INFRASTRUCTURE (PKI)

PKI strengthens authentication by supporting the distribution and identification of public encryption keys. This makes it possible for users and devices to securely exchange data over networks, such as the Internet, and to verify and authenticate the identity of the other party. Digital signature is one function enabled by PKI and used to address the problems of tampering and impersonation in digital communications. PKI also affords government to go beyond pure identifications, helping to step into seamless Government-to-Citizens and Citizens-to-Government information flow while reducing operation cost.

MULTI-FACTOR AUTHENTICATION

This refers to the use of at least two criteria for proof of identity. Multi-factor authentication helps prevent fraud and unintended access to data stored on the document. The strongest form of authentication uses all three of the factors shown in the table.

SOMETHING YOU HAVE

This is the eID itself. If this is the only factor used for authentication, then simply presenting a stolen card is all that's needed to access services.

SOMETHING YOU (AND ONLY YOU) KNOW

This is typically a PIN number you enter into a keypad built into the reader. Newer technology is making it possible to type the PIN onto the card itself. PINs and other types of passwords add a level of security, but they can still be shared, copied, or stolen.

SOMETHING YOU ARE

This is a physical characteristic of you as an individual. Commonly referred to as a biometric, it's often a fingerprint, but can also be a facial scan, an iris scan, or some other proven measure of individuality. Biometrics are extremely difficult to copy or fake, and make for robust authentication. When used in combination with the other two factors, biometrics deliver a very high level of security for authentication.

Building a strong security architecture helps minimize the risk of tampering and misuse once the card is issued but, as it turns out, many of the primary security risks for an eID program are not related to use of the eID, but its creation. The next section looks at the recommended security measures to be taken at each step, from enrollment to issuance.

ANTICIPATE VULNERABILITIES: EVALUATE THE PRE-ISSUANCE PROCESS

Assuming the **eID architecture** has received the necessary security certifications, and the document itself has been properly issued, the risk of hacking while it's in circulation is very small. Criminals are often deterred from mounting attacks on cards that have already been issued, because the effort involved is usually much bigger than the reward.

Deploying a solid security architecture on the card itself is a vital part of the process, but the card architecture doesn't address vulnerabilities in the stages of the card's production. To identify potential vulnerabilities during the pre-issuance process, it's important to consider each step in the eID's creation. The table summarizes the risks most commonly associated with each stage of production, and the methods to be put in place to mitigate those risks.

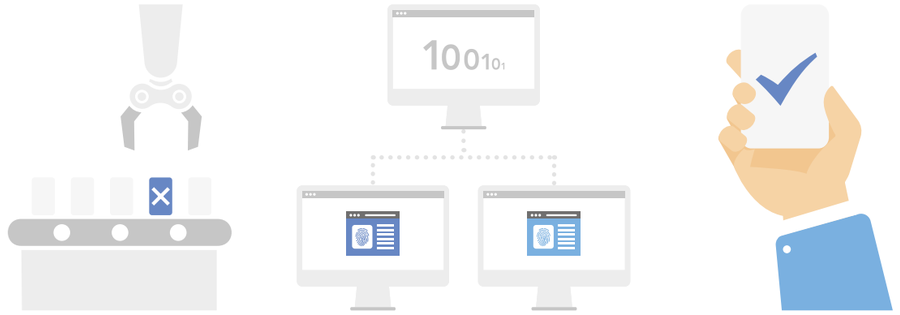
THE PRE-ISSUANCE PROCESS

ENROLLMENT

Perhaps the most important step in the creation of an eID, the enrollment stage is used to ensure the completeness and veracity of information provided by the citizen. Sometimes referred to as the "proofing" stage, this is when people apply for an eID and supply proof of identity.

DEDUPLICATION

At this stage, enrollment data is compared to existing data to identify and remove duplicates. This is usually done with a 1:N biometric search in an AFIS database.



PRODUCTION

During manufacturing, the goal is to deliver quality-assured cards that are ready for personalization. Track blank cards throughout the process, so that any lost or stolen cards can be blacklisted before they're loaded with data and put into circulation.

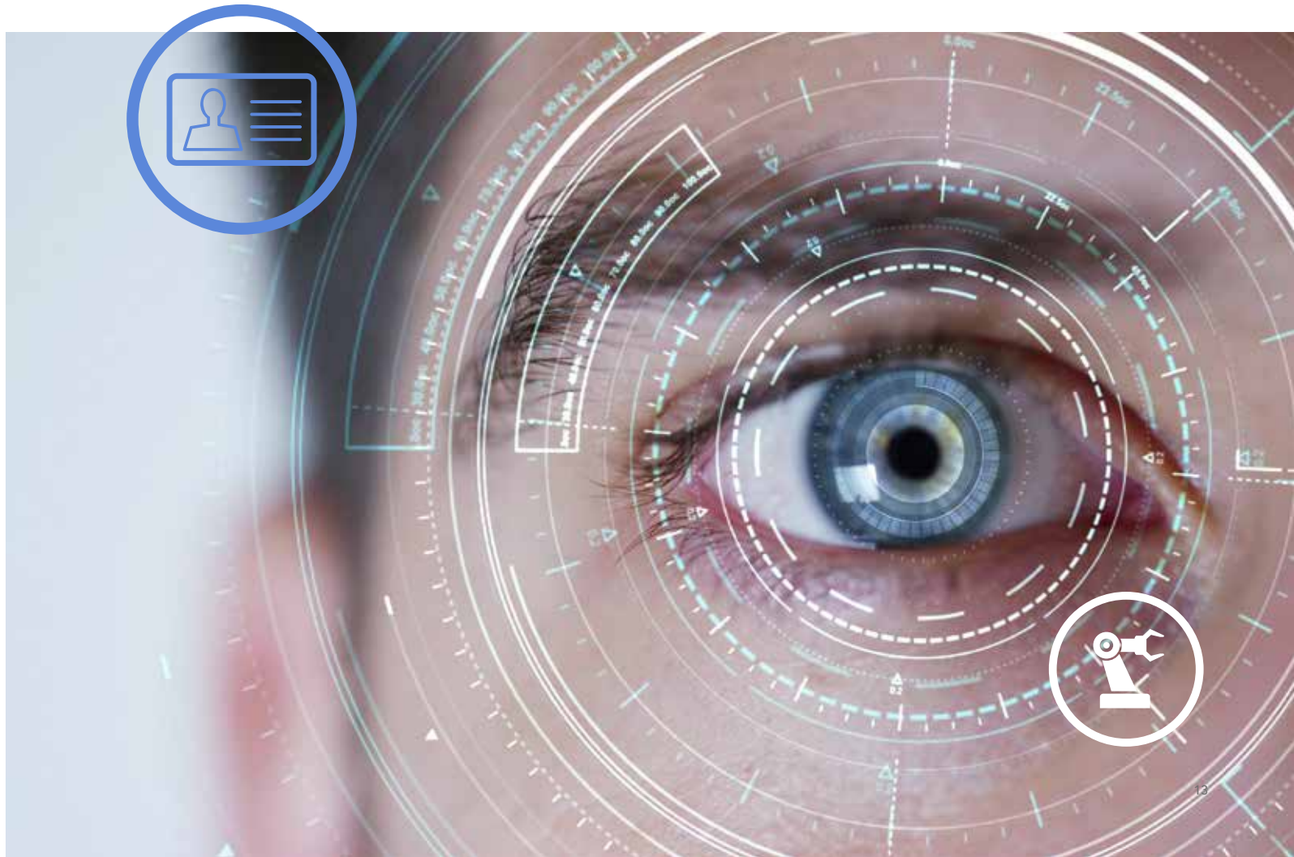
PERSONALIZATION

Deploy job sharing so that no single person is authorized to encode blank cards. Also ensure privacy by only encoding properly approved data.

ISSUANCE

Before issuing the card, ensure that the information is correct by having citizens check their personal data, and confirm that the citizen is indeed the owner of the card by matching their biometric data to that stored on the card. Once the card is issued, activate it in the card-management system.

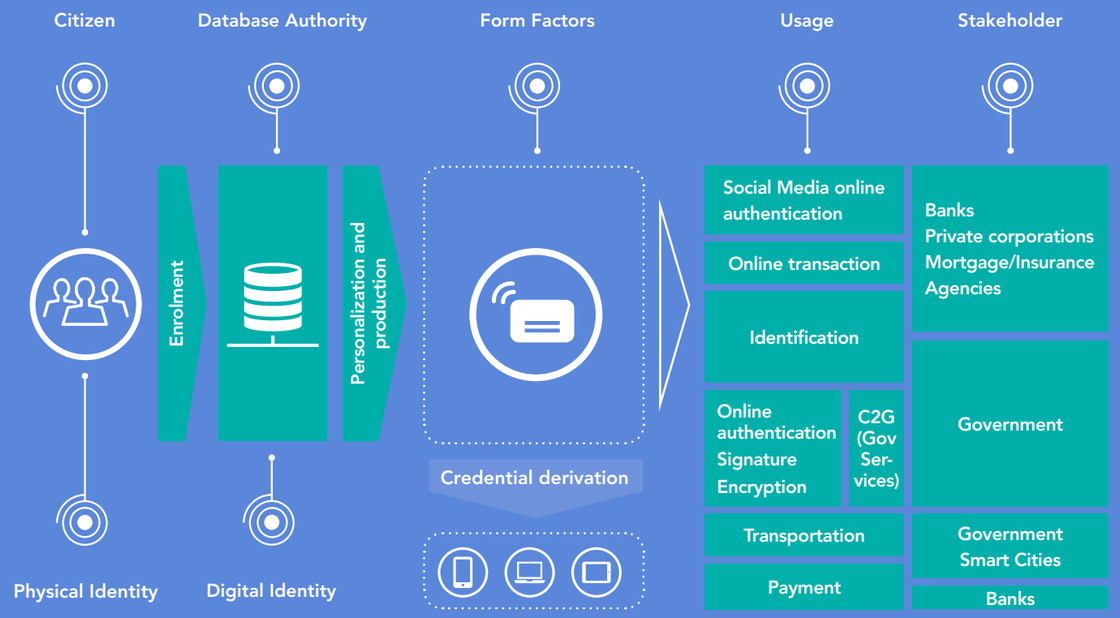
Minimizing risk during the pre-issuance phase is just one aspect of creating an eID system solution. The next section builds on the points given in the table, by offering considerations for establishing the overall program.



PUT THE PIECES IN PLACE: IMPLEMENTING THE eID SYSTEM SOLUTION

Developing the **overall system solution** is another time for careful planning, so as to increase efficiency, avoid unnecessary delays, and reduce the duplication of effort. A carefully designed solution increases return on investment by streamlining steps, simplifying processes, and lowering overall cost.

The image below gives an overview of the system solution that typically governs issuance and field use.



- **Physical Identity:** Physical Citizen
- **Digital Identity:** Electronic counterpart of Physical Identity
- **Credential:** Cryptographic and/or biometric token linked to your Digital/Physical Identity
- **Form Factor:** Secure Device carrying the Credential

The rest of this section lists things to think about when assembling a typical system solution. The specifics will, of course, vary depending on the use cases and business models defined when creating the baseline configuration, so this should only be viewed as a starting point for discussion and not a complete set of considerations.

CIVIL REGISTRY

Having a civil registry, or a nationwide database of citizen information, makes it easier to know who is eligible to receive an eID, access services, and enjoy other rights of citizenship. In 1990, the UN Convention on the Rights of the Child proclaimed it a human right to have one's identity registered at birth (so as to assert citizenship), and the goal of having a civil registry in every country is part of the UN's agenda for 2030.

INDEPENDENT CONTROL

Civil registries are typically managed by an independent agency, guided by a formal legal and administrative framework.

CENTRALIZED OR DECENTRALIZED

A civil registry can use either format, depending on the country's traditional organizational structure, but a centralized approach enables easier maintenance and greater control over the entire system.

DIGITAL DATA

A digital platform is essential for efficiently managing data and enables integration with and connection to both public and private institutions which deliver services. Where legislation allows, it's recommended to issue a unique Personal Identification Number (PIN) at the time of birth, and combine the PIN with a biometric for secure authentication. Adding biometric capabilities, with an Automated Fingerprint Identification System (AFIS), is strongly recommended. Not only does AFIS add an extra level of security, it can add utility to the database, too, by giving other agencies, such as law enforcement, access to the information.

BASELINE INFORMATION

Specific information logged in the registry will vary, but typically includes things like name, gender, date of birth, address, date of death, parents, children, list of other documents issued, and so forth.

ENROLLMENT CENTERS

These are brick-and-mortar locations that are properly staffed and equipped with the tools needed to support a smooth, efficient, and cost-effective enrollment process.

FOCUS ON QUALITY AND DEDUPLICATION

Emphasize identity proofing and the capture of digital data only. This ensures quality of data and enables deduplication of the system.

EVALUATE COVERAGE

Manage the trade-off between regional offices and the effort citizens need to expend to get to enrollment centers. The cost of equipping and operating enrollment centers can add up quickly, so consider mobile enrollment stations as a way to cover more areas more effectively, especially in remote regions.

PRODUCTION OF EIDS

As mentioned in the section on mitigating risk during the pre-issuance process, it's important to implement stringent security practices for the production, shipment, storage, accounting, and destruction of blank smartcard documents.

TRACK CAREFULLY

Using a comprehensive tracking and numbering system to identify individual documents at every step of the issuance process, from production to personalization.

MAKE VERSUS BUY

The decision to outsource production is usually dictated by volume. A government agency that will be producing eIDs in large volume can probably justify the cost of in-house production, but a smaller agency, facing smaller volumes, is probably better off using a third-party partner or a non-government facility.

ISSUANCE

Customer service and ease of use are important considerations for the issuance process.

CONVENIENCE VERSUS SECURITY

Consciously manage the trade-off between instant issuance and issuance process security. Optimize the process for fast, citizen convenient but secure issuance. Combining enrollment and issuance centers can increase convenience while lowering overall cost.

PERSONALIZATION

Maintaining high security is one of the most important factors in effective personalization.

TIGHT CONTROL

Limit access to personalization facilities; establish staffing structures and operating environments that prevent unauthorized entry.

CENTRALIZED VERSUS DE-CENTRALIZED

Manage the tradeoff between highly secure, centralized personalization and less secure, de-centralized personalization, keeping in mind the costs associated with each approach, and the citizen's need to travel to personalization facilities.

QUALITY ASSURANCE

Create a personalization process that ensures the highest possible quality, for final documents that are pristine, safe to use, and fully interoperable.

IT INFRASTRUCTURE

The card readers, computer networks, and software components, along with the personnel needed to install and maintain them, are key to an effective deployment, but can also add cost.

STAY MODULAR AND OPEN

Control costs by using a modular, open architecture that support step-by-step deployment of predetermined use cases, in line with present and future business models.

OPTIMIZE SYSTEM COST (TOO THIN)

Choose an operating model that minimizes your system implementation and maintenance Advance planning helps identify what resources will be needed and when, for more manageable project costs.

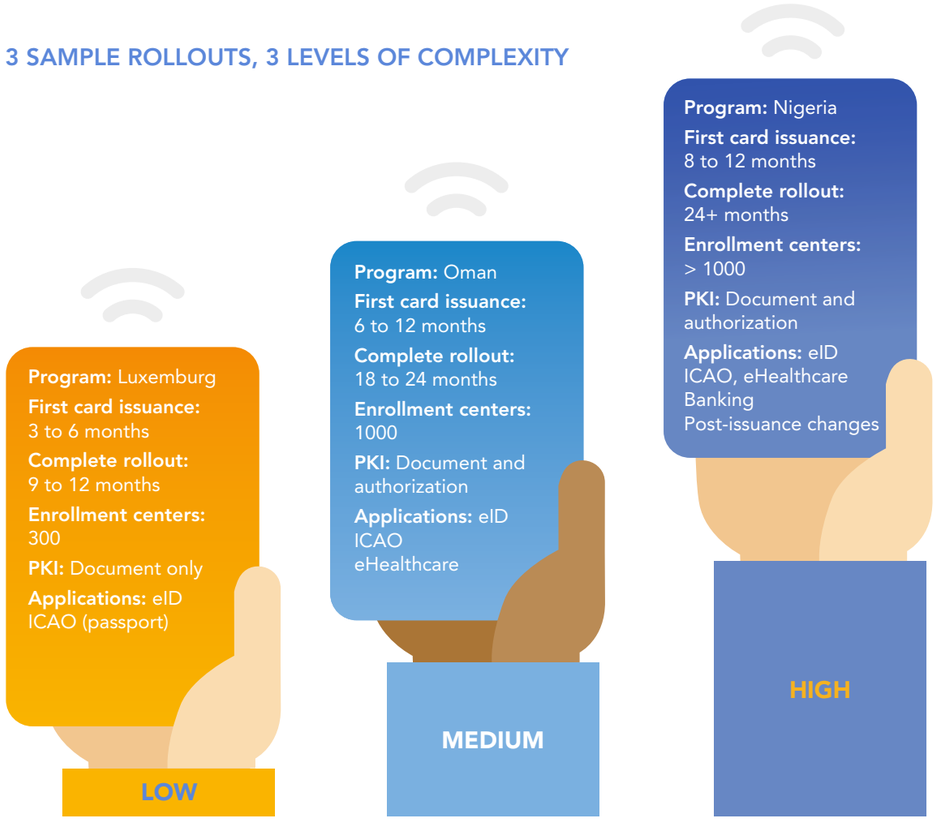
The next section gives three successful real-world examples of eID projects that put these considerations into practice.

THREE REAL-WORLD ROLLOUTS

The following three examples are actual projects supported by NXP and show the factors that typically influence project **complexity**.

Each country followed a process similar to that described above, beginning with the creation of a civil registry and enrollment centers. All three projects outsourced card production, and began with centralized, laser-based personalization. The differences in complexity had to do with the number of enrollment/issuance centers, the extent of the PKI implementation, and the number and type of applications being deployed.

3 SAMPLE ROLLOUTS, 3 LEVELS OF COMPLEXITY



In all three cases, government agencies worked with NXP and other deployment experts to create a solid technical foundation for their eID programs. Each project emphasized the importance of defining use cases in detail, before any development took place, so as to make sure the eIDs performed as expected and provided the greatest benefit to everyone involved. Each project also made it a high priority to establish a full system solution ahead of time, so as to have a smooth process for producing, issuing, and managing eIDs before they went into circulation.

FINAL THOUGHTS

There are strategies for strengthening security, reducing cost, increasing effectiveness, and maximizing ROI at every stage in the eID process.

Bringing the eID vision in line with other government initiatives can take time, but there's lasting benefit to beginning with a process that identifies synergies, overlaps, and opportunities for collaboration. By working together toward a common goal, government stakeholders can save time and effort while introducing fit-for-purpose programs that will garner widespread support.

Admittedly, it can be hard to anticipate the long-term needs of different government stakeholders and to bring everyone into alignment. That's part of why it's so important to have a sound technology platform in place, with enough built-in flexibility to allow for changes over time and meet future needs. Breaking the deployment down into stages, instead of launching everything at once, is another way to work around any gaps in alignment. Introduce the pieces that everyone agrees on first, while continuing to foster stakeholder support.

Executing a clear communication plan, to articulate the eGovernment vision and explain how the eID program supports that vision, can help increase stakeholder support, especially within the citizen community. Making it clear why eIDs are being developed, and how people will benefit from their use, can generate support for the program and put the agencies involved in a positive light.

Perhaps the most important thing to keep in mind, though, is that there's no need to go it alone or reinvent the wheel. The smartcard technology used to support eID functions is proven and widely trusted, the infrastructure expertise needed to design and deploy eID programs is readily available, and the growing number of countries with eID programs in place means there's a broad body of knowledge, supported by a base of established best practices.

With some careful planning, a long-term commitment to establishing eGovernment processes, and the right team of experts, implementing a nationwide eID program can create a quantifiable, sustainable return on investment.

To learn more about how NXP helps countries design, develop, and deploy eIDs, contact our sales offices or visit **www.nxp.com/smartgovernance.**