BIRTH CERTIFICATES

RECOMMENDATIONS FOR BIRTH CERTIFICATE SECURITY

The commercial, academic and government members of the Document Security Alliance have teamed together to provide an informative summary of the social and technical factors that influence fraud related to Birth Certificates. We now stand prepared to provide assistance and answer questions to help government organizations improve the security of their documents.

Contents

DSA
DOCUMENT SECURITY ALLIANCE

EXECUTIVE SUMMARY

DSA recommends that federal and state governments acknowledge and embrace the importance the birth record serves in the identity chain and address improvements to its physical security and the issuance process. All U.S. birth certificates should incorporate overt and covert anti-counterfeiting technologies to increase the security of the document against counterfeiters.

Vital Records capture key elements of personal identity: name, birthplace, birth date, and parents' names. These documents are used by issuers in the public and private sectors to establish the individual's identity when new government identification documents are created and issued.

Birth certificates are often called breeder or source documents since they facilitate the acquisition of additional identity documents. Starting with the birth certificate, one can breed other documents, such as a Social Security card, driver's license or passport. Most birth certificates are certified copies or abstracts of the actual birth record, which is filed and maintained in the local jurisdiction of birth.

Currently, 6 states allow open access to birth records at the state or local level and release informational copies to anyone who requests them. Imposter and identity fraud often begins through such access.

In 2005, the National Association for Public Health Statistics and Information Systems (NAPHSIS) recommended cross-matching birth and death records to reduce identity fraud. Many vital records offices lack the automation resources to perform this match in a timely fashion, creating loopholes that are exploited by criminals. While some states have an inter-jurisdictional exchange program to exchange birth and death records, not all states have appropriated the funding necessary to take full advantage of the system.

NAPHSIS has developed the Electronic Verification of Vital Event (EVVE) system to provide government-to-government verification of birth and death information. The system is currently available in 53 states and territories.

Given the public's concern about identity theft and the misuse of personal information, legislators and government officials will need to ensure that broader exchanges of identity information are not compromised.

It is in the interest of all government agencies to procure products and services that meet current security standards. To this end, DSA recommends that all birth certificates include advanced counterfeit deterrent features and that any organization in the birth certificate issuance supply chain comply with the American National Standards Institute/North American Security Products Organization (ANSI/NASPO) Security Assurance Standard.

STUDY & RECOMMENDATIONS

Almost everyone carries a means of personal identification. Some carry multiple identity documents – typically as credit-card sized cards, each associated with a specific set of permissions. Some may be used to gain physical access to a school or workplace; others provide logical access to data in a computer or personal account at a financial institution.
Though offered and often accepted as proof of identity, these cards are more appropriately understood as tokens of identity. They are but one of three basic building blocks to authenticate a person's identity. The three blocks are:

1) What a person has in his or her possession, such as a passport, driver's license or birth certificate

2) What a person knows, such as a Personal Identification Number (PIN), password or elements from personal or family data that outsiders would be unable to determine

3) What a person is or does, including personal or behavioral characteristics as varied as fingerprints, retina or iris images or the dynamic pattern recorded when someone walks or pens a signature.

These building blocks serve to reinforce personal identity and reduce the risk that an imposter will succeed in usurping an individual's identity. When a document such as a driver's license is structured with all three building blocks, it protects both the person who carries the document and those who rely on the document to authenticate the individual.

An overarching problem with many of the documents used to assert identity is that they were originally issued with relatively little thought to security. Birth certificates are completed by county or city officials to record births within their jurisdiction. Social Security cards provide individuals with a number to record their contributions to Social Security and, ultimately, to apply for benefits under the program. Over time, these credentials have been accepted to assert identity when the individual applied for a driver's license or passport.

Identity-related crimes are on the rise, and existing penalties appear insufficient to deter criminals. Stronger processes and deterrents are needed if we are to rebuild the foundations of identity for our citizens and put protections into place that will thwart criminals as well as terrorists. These changes will require the coordination and cooperation of multiple organizations and the enactment of appropriate legislation at each level of government.

DSA recommends upgrading the security of breeder documents through the use of advanced counterfeit deterrent features, cross-jurisdictional authentication, cross-database application verification, and systems for facial recognition. DSA also recommends upgrading issuance, authentication and verification processes.

1. PROBLEM AREAS

To those experienced and involved in document security it comes as no surprise that the incidence of birth certificate related fraud is as high as it is. Indeed, it may even be higher than official reports indicate because a large proportion of counterfeit and falsified certificates go undetected due to the lack of deterrent power inherent in many past and present certificates. The major factors we have identified include:

- No direct linkage between the person and the record - There is nothing in birth records that positively link the record to the unique characteristics of the person. The holder of a copy of a birth record is therefore able to claim to be the person without fear of rebuttal.

- Open Access – Several states have laws that classify Birth Certificates as public documents, available to anyone. These states are too often a portal to identify fraud.

- Lack of Consistency - With over 6400 issuers and 14,000 versions, quality examination and authentication is beyond the realm of normal human capability. To make matters worse, most examiners responsible for document authentication do not have the benefit of exemplars or samples for comparison and thus have no basis for evaluation / adjudication.

- Historically Non-secure - Records of birth and death kept by the vital records offices of state health departments have, until recently, not been treated as identity documents.

Accordingly, their storage, retrieval, copying and issue have not always been securely managed by all jurisdictions. Some have responded to several prior acts (such as the Illegal Immigration Reform & Immigrant Responsibility Act of 1996) with upgrades in both document and issuance security but others have not. Security is inadequate in too many jurisdictions.

Given the multiple problem areas that exist, DSA recommends a comprehensive education program be rolled out to states and local jurisdictions to inform about the problem, ramifications from lack of corrective action and how to address them.

2. IMPACT

Crime based on identity theft and document fraud permeates many aspects of our society, injuring government, business and individuals alike. Today, the collective annual cost of this theft and fraud in the United States is hundreds of billions of dollars. The cost is not solely monetary. As the events of 9/11 revealed, even seemingly minor problems can quickly become national in scale. Identity fraud damages consumer confidence and erodes the ability of business and government to provide vital services. Citizens directly impacted by these crimes are not only outraged; they look to government agencies and business organizations for solutions.

Birth certificate fraud was the subject of a year 2000 report by the Department of Health and Human Services Office of the Inspector General. This pre-9/11 work represents the most thorough investigation of the problem reported to date and we believe that the vast majority of the findings and conclusions presented remain valid in the post-9/11 era.

Dominant in this report was the finding that 85-90% of fraud detected by the Immigration and Naturalization Service (INS) (now U.S. Citizenship and Immigration Services) and passport services staff was the result of imposters making use of genuine birth certificates either stolen or acquired from others.

Today, the U.S. Department of Education, Office of Inspector General provides a number of recommendations to protect against identity fraud, including not carrying "your Social Security card or birth certificate with you".

Identity fraud has become pervasive throughout the United States. Since non-secure birth certificates substantially contribute to this problem, DSA recommends requiring that all jurisdictions issue birth certificates that incorporate advanced anti-counterfeit deterrents and that they be produced by vendors who are in compliance with the ANSI/NASPO American national security assurance standard.

3. CRITICAL NEEDS

The problems and impact of identity fraud are clear and seldom argued. Key changes that will mitigate identity fraud include:

- Implementation of a uniform security assurance standard, and auditing to that standard, by all birth certificate issuing operations.
- Standardizing the process of identity verification at all issuing agencies before re-issue of an authentic credential.
- Establishing minimum document security standards for all birth certificates issued nationwide.
- Linking the birth record to the individual with unique biometric and/or life history identifiers, and limiting the period of validity of the certificate if age dependent identifiers such as a photograph are used.
- Raising the physical security of the birth certificate document to at least equal the security of documents it breeds.
- Issuance controls that limit access of legitimate birth credentials to only those whom the credential represents or their legal custodians.
- Improving interstate cooperation, data access and sharing of state Vital Record and Motor Vehicle information.

DSA

4. RECOMMENDATIONS

The DSA recommends the following actions to improve Birth Certificate security:

1. Acknowledge the problem now! Solutions to adequately improve the security of identity credentials are complex and will require time and coordinated efforts to fully the problem.

Whenever security-sensitive materials or technologies are being procured by government agencies, DSA recommends requiring that vendors comply with national security assurance standards.

2. Engage all interested parties (not just Birth Certificate issuers but examiners at both federal & state levels, law enforcement, and down-stream document issuers) in the definition of design and performance characteristics of an improved Birth Certificate document.

3. Develop and implement a nationwide minimum common document issuance standard – to establish a direct link between access of birth credentials which may be used to establish identity, and the individuals whom that credential represents.

4. Develop and implement a nationwide minimum common document security standard – to include use of common advanced counterfeit deterrent features - for all Birth Certificates issued.

5. Require implementation and Level III (minimum) conformance to the U.S. ANSI/NASPO-SA-2008 Security Assurance Standard for all participants in the Birth Certificate issuance supply chain.

6. Introduce and encourage the implementation of a mechanism or metric that links the Birth Certificate document to the individual it purports to represent.

7. Improve access to, and utilization of, electronic verification systems. EVVE deployment is a valuable first step in cross-jurisdictional sharing of pertinent birth data, but until all involved parties utilize this information significant vulnerabilities will remain and continue to be exploited by nefarious elements of society.

DSA recommends that federal and state governments embrace the importance the birth record serves in the identity chain and address improvements to its physical security and the issuance process. All U.S. birth certificates should incorporate overt and covert anti-counterfeiting technologies to increase the security of the document against counterfeiters.

5. CONCLUSION

Simple, effective, and economical solutions are available today to reduce the proliferation of fraudulent Birth Certificates. Yet, problems persist, in part, because organizations accustomed to "business as usual" resist examining or changing current practices. The challenge is not technology or even cost, but getting the people and organizations responsible for issuing these sensitive documents to take steps to analyze current practices and determine how to improve the security of the documents they generate and use.

DSA
DOCUMENT SECURITY ALLIANCE

204 E Street, NE
Washington, DC 20002
Phone: 202/543-5552
Fax: 202/547-6348
www.documentsecurityalliance.org
info@documentsecurityalliance.org

The Document Security Alliance (DSA) is a not-for-profit organization focused on document security at all levels of government to enhance our nation's economic, personal, and homeland security for the 21st century. DSA's goal is to leverage our government and industry members' expertise to identify methods of improving security documents and related procedures to combat fraud, terrorism, illegal immigration, identity theft, and other criminal acts.