Multi-factor Authentication Reference Materials

Collection of References that touch on various aspects of Multi-factor Authentication

These are a variety of documents that might be of some value to the MFA Cohortium and Pilot efforts.

Multi-factor Authentication Integration Strategies

- SURFnet Step-up Authentication-as-a-Service: A study of the architecture and processes.

File	Modified
PDF File rapport_Step-up_Authentication-as-a-Service_Architecture_and_Procedures_final.pdf SURFnet: Step-up Authentication-as-a-Service - A study of the architecture and processes.	Feb 17, 2013 by Michael Grady (unicon.net)

> *The need for stronger forms of authentication is felt by Identity Providers (IdP) within the SURFconext federation. A business case analysis performed by SURFnet in Q2 2012 shows a clear need among SURFnet's constituency to address this need by introducing a service in the SURFconext environment that offers strong authentication on top of the existing identity hosted by a user's home institution. This report is a study of the architectural and procedural aspects of introducing such a service.*
> *A number of current and near future use cases (described in Chapter 1) have emerged for which username/password is no longer sufficient. These use cases are in the areas of student information systems, administrative systems, and in collaborative research in which privacy sensitive and/or medical data is handled. The need for better authentication can be effectively addressed by introducing a SURFnet operated service (referred to as "SURFsure" in this report) offering technical and organisational assistance to the IdPs.*
> *Handling different Levels of Assurance (LoA, the confidence relying parties can have in the authenticity of an identity) within a federation must be based on open and accepted standards. While some of these standards are still under development, it is already possible to make future-proof choices for standards defining the semantics and communication of the LoA. The SURFsure service architecture described in Chapter 2 supports the signaling of the LoA within the SURFconext federation while at the same time remaining loosely coupled to SURFconext.*

Higher Education Specific

- Top Ten Applications for MFA in Higher Education
- Information Security Guide: Effective Practices and Solutions for Higher Education: Two-Factor Authentication (2011)
  About halfway through this document, one will find the Results from the 2011 Internet2/InCommon Survey on Campus Use of Two-Factor Authentication.
- Multifactor Authentication Approaches and Multifactor for InCommon Silver (2012)

> *Multifactor authentication (also referred to as two-factor authentication) adds another level of complexity and security to a password-only arrangement. Interest in multifactor continues to grow, as some federal agencies move in that direction. InCommon has added service offerings in this area, as well, and some schools now plan to use a second factor as a way to meet the requirements of the InCommon Silver Assurance Profile. Join our speakers to learn the basics about multifactor authentication, the pros and cons of different approaches to multifactor, and how one campus plans to use this approach for InCommon Silver*

- Multifactor Authentication in Higher Education (2011)

> *The classic case for multifactor authentication is the need for higher-assurance authentication for transactions that expose the institution to significant risk. Another driver is the desire of some end-users and system administrators to self-select for heightened security. The U.S. Department of Education plans to require two-factor authentication for assets that are part of the Federal Student Aid program. Join us for an overview on the topic and participate in a discussion of business drivers, technology options, potential barriers, and current implementations of multifactor authentication.*

- Information Technology in Higher Education: 2010 Survey of Chief Information Officers

> *A substantial number of institutions either have (11 percent) or are considering (47 percent) implementation of multifactor authentication solutions as part of their security plan. ... Among the solutions mentioned were Safeword, VPN, PKI USB, Active Directory, SecurID, IBm Tiviloi, CISCO, CAC readers, LDAP, and microsoft SmartCard.*

- Information Security Guide: Effective Practices and Solutions for Higher Education: Two-Factor Authentication (2011)

> *The Information Security Guide: Effective Practices and Solutions for Higher Education (referred to as "the Guide") is, as its subtitle suggests, a compendium of information providing guidance on effective approaches to the application of information security at institutions of higher education. It is a key publication of the Higher Education Information Security Council (formerly the Security Task Force). Its content is actively maintained by a large group of volunteers who are information security practitioners at a variety of colleges and universities.*

This is the section focused on two-factor authentication, including presenting the various technology approaches, the business reasons for such, and the results of the 2011 Internet2/InCommon Survey on Campus Use of Two-Factor Authentication.

- Educause Identity Management in Higher Education, 2011 ECAR Research
  Shorter Roadmap: http://net.educause.edu/ir/library/pdf/ERS1101/ECM1101.pdf (above document is 137 pages, Roadmap is only 4 pages)

> *Authentication:*
> *The starting point for IdM is authentication--- determining who a user is---and our data show good progress in several key aspects of authentication. Since 2005, the use of strong passwords increased from about 60% to about 75%, and responding institutions that prohibit the use of unencrypted passwords rose from less than 30% to nearly 60% in 2010. Mandating that electronic identifiers never be reassigned also strengthens authentication, and use of such "unique for all time" IDs climbed by a third.*
> *Institutional policies specify what proof users must furnish when they apply for electronic credentials, and in cases where a credential will provide access to sensitive systems, an institution might set a higher threshold for such identity proofing. In our research, however, fewer than 30% of respondents said they do this now, and only another 20% plan to. We also saw little change in adoption of public key infrastructure (PKI) or of multifactor or biometric authentication.*
>
> *In the early years of this century, public key infrastructure (PKI) showed promise as a tool not just for authentication but also for ensuring the integrity of information trans- ferred between automated systems. Our 2010 survey found that interest in PKI had increased slightly since 2005 but that it was still rarely adopted, with fewer than 2 in 10 respondents reporting its use. More important, though, the future of this technology seems limited. Within the longitudinal sample, respondents saying they had no plans to implement it grew from 2 in 10 in 2005 to 7 in 10 in 2010.*
> *In 2010, multifactor approaches to network authentication other than PKI, including one-time passwords, were being used at fewer than 2 of 10 respondent institutions, and about half the institutions reported no plans to use them. Biometric identification was in use at fewer than 5% of respondent institutions, and most of the remainder reported no plans to use it.*
>
> *Token-Based Authentication Methods*
> *Our survey asked several questions relating to token-based authentication. We've already discussed token-based PKI, which only 5.9% of institutions reported using and nearly two-thirds indicated they are not planning to use.*
> *We also asked a question about one-time password (OTP) tokens (such as the SecurID product sold by RSA). These sorts of systems display a string of characters that generally change over short periods of time (e.g., 60 seconds). The user enters the displayed string, usually along with an ID and secret PIN or password. The string is then compared with a string of characters generated by a synchronized authentica- tion server. If that matches, along with the ID and PIN/password, the user is authen- ticated. One-sixth of responding institutions said they were using such technologies, and another one-tenth indicated that they were planning to use them. On the other hand, a substantial majority responded that they do not plan to use OTP technology. This is one of the multifactor methodologies discussed earlier in this chapter (in this case, two-factor authentication).*
> *Multifactor authentication implies the use of some sort of token or biometric factor. Because usage of the latter was reported at fewer than 1 institution in 20, we know that most of the 15.2% multifactor usage is relying on some sort of token as the second factor. Using this technology typically requires the user to enter an ID and a password/PIN, and to insert a token into some sort of reader (e.g., by inserting a USB flash drive that contains some sort of digital certificate into a USB slot). Three-factor authentication must be relatively rare in higher education, since it almost always implies the use of biometric factors (something you are) in addition to tokens (something you have) and passwords (something you know)--- and we already know that biometric factor authentication is very rare.*
> *One reason that token-based authentication (and, therefore, multifactor authen- tication) is not being used widely for network access is its cost. The initial cost to buy and deploy tokens widely, as well as to create the infrastructure to support the technology, is relatively high. Likewise, the support costs for training, trouble- shooting, retiring tokens for people who leave, replacing lost tokens, etc. are also a burden. In addition, digital certificates (used in single-factor authentication) sometimes suffer from some of the same weaknesses as password authentication. Since many certificates are stored in computers, which themselves are protected by password, criminals with access to the user's machine may be able to overcome that password and therefore use the digital certificate.*
> *Some institutions choose to use these technologies selectively---only where the risks are very high and the number of users is small; this keeps the cost manageable. For example, two-factor authentication is used by some institutions for a small set of network or system administrators as the authentication mechanism allowing them to access sensitive infrastructure elements like routers and key servers.*

Sample campus-specific documents related to MFA (e.g. RFPs, Strategic Plans)

- UNIVERSITY OF MARYLAND UNIVERSITY COLLEGE REQUEST FOR PROPOSAL # 91029 FOR MULTI-FACTOR STUDENT AUTHENTICATION PRODUCTS AND SERVICES (August 2012)

> *8.1 DESCRIPTION/PURPOSE: The University is seeking multiple solutions for authenticating the identity of students who register for and participate in online courses and programs. The University may or may not purchase all authentication solutions submitted by a Proposer for consideration, so the proposed products and/or services must not be dependent on each other for functionality and must be able to be purchased separately.*
> *8.2 MULTI-FACTOR IDENTITY FUNCTION: The University currently protects student identity via secure login/passwords by utilizing single sign-on architecture. UMUC is seeking to enhance this architecture by utilizing multi-factor security functions with more than one means of authenticating identity.*
> *8.3 DATA COLLECTION AND STUDENT PRIVACY: UMUC is committed to protecting the privacy of students and the security of their personal data. The University is seeking a solution that its students will not perceive as intrusive or an encroachment on their privacy.*
> *8.4 SCALE: The University of Maryland University College is a global institution with students and faculty located in the United States, in Europe and Asia, and other parts of the world.*

- Stanford IT Services Strategic Plan (2011)
  - Page 5:

    > *AUTHORIZATION AND IDENTITY SERVICES - IT Services will **offer twofactor authentication**, along with strong identity binding processes to support the secure and efficient use of smart devices, mobile client platforms, and cloud services. This will create a level of assurance sufficient to meet non-repudiation standards.*

  - Page 8:

    > *IT Access and Privacy*
    > *Deliver tools and services to secure university electronic resources*
    > *o FY2011 Implement Managed Desktop Services and Mobile Device Security; **Offer Multifactor Authentication** and Account Abuse Detection*

MFA Technologies and whitepapers

- Information Security Guide: Effective Practices and Solutions for Higher Education: Two-Factor Authentication (2011)
  The first half of this document describes what two/multi-factor authentication is, and provides a reasonably extensive summary of all of the methods and technologies to providing additional authentication factors, including security tokens, smart cards, biometrics, and "second channel authentication - mobile phone-based" approaches.
- Phone-based Multi-factor Authentication Vendors
- Duo Security: Top 7 Reasons Companies Don't Use Two-Factor Authentication (Dec 2012)

> *In the spirit of year-end reviewing and wrapping up, we've been conferring with the ghosts of security trends past, present, and future. One of the most notable trends we've seen is that 2012 was the year in which two-factor authentication really broke out of the security community and became part of the broader conversation about everyone's online account security.*
>
> *Just to illustrate, the Google Trends graph to the right shows search interest over time in the phrase "two factor authentication." That spike in August 2012 is Mat Honan's well-chronicled epic account hack and since then the baseline level of interest in two-factor authentication has been nearly twice as high as it was before.*
>
> *Knowing what we all know now about how vulnerable our digital lives and our personal and company data are to hacking and account takeover, the key question really isn't "Why do companies need to add two-factor authentication?" but "Why hasn't every company added it already?"*
>
> *Here's a roundup of seven of the objections to implementing two-factor authentication that we routinely hear. If any of these sound like your company, talk to us about how easy two-factor authentication can be.*

- Guide to Evaluating Multi-Factor Authentication Solutions
  (Note that there is a vendor-bent to this, as whitepaper produced by PhoneFactor, a vendor with a multi-factor phone-based solution. And just bought by Microsoft in October 2012.)

> *Passwords are a known weak link and continue to be exploited at alarming rates. From simple phishing schemes to sophisticated, targeted phishing attacks, gaining access to a user's password is an easy and prolific attack. Regulatory agencies agree and are setting increasingly rigorous requirements for strongly authenticating users. Multi-factor authentication is no longer optional for many organizations.*
> *Whether you're planning to implement multi-factor authentication for the first time or are looking to expand or upgrade your current implementation, this whitepaper will help you choose the solution that is right for your business. Key evaluation criteria will be defined and the most prevalent multi-factor authentication methods, including hardware tokens, smartcards, certificates, and PhoneFactor's phone-based authentication will be evaluated against the criteria.*

Regulatory and policy examples where use of MFA is specified

- U.S. Department of Education Privacy Impact Assessments (PIA)

    - A number of these PIAs specify that multi-factor authentication is used as one of a number of risk mitigation measures to minimize privacy risks. And these PIAs are an interesting instrument to consider in assessing the sensitivity of the data/information that is collected /handled and laying out the risk mitigation strategies. Might consider how something like this should factor into our work.

- Understanding the Security & Privacy Rules associated with the HITECH and HIPAA Acts: Topic: Multifactor Authentication (2011)

> *The Health Information Technology for Economic and Clinical Health (HITECH) Act requires covered entities and their business associates to comply with new guidance related to security and privacy of Protected Health Information (PHI). The Health Insurance Portability and Accountability Act (HIPAA) was recently strengthened via Security and Privacy Rules issued by the Centers of Medicare and Medicaid Services (CMS).*
> *The purpose of this paper is to examine the regulations, rules and guidelines for one aspect of security and privacy, multifactor authentication. The goal of this paper is to aid organizations in decisions regarding implementation of security and privacy protections to support access to health information or electronic health records (EHR).*

- Pivot Group - Multi-Factor Authentication: What You Need to Know

> *The Federal Financial Institutions Examination Council (FFIEC) has issued guidelines for safeguarding high risk transactions, such as online money transfers. The confidentiality, integrity, availability, and non-repudiation of customer information must be protected. The guidelines mandate that financial institutions develop an appropriate security program by utilizing a risk assessment, then use authentication appropriate for the level of risk.*
> *The FFIEC states that single-factor authentication is clearly an unacceptable control mechanism for high risk transactions involving personally identifiable customer information. Hence, it is suggested that multi-factor authentication, multi-layered (defense- in-depth) security, and other controls reasonable to mitigate risk be implemented.*

Various whitepapers on MFA, risk & market analyses, etc.

- The Adoption of Single Sign-On and Multifactor Authentication in Organisations – A Critical Evaluation Using TOE Framework (2010)

> *The proliferation of user credentials for system access coupled with the resulting rising security threats have led to the development of single sign-on (SSO) access control and multi-factor authentication (MFA) technologies. This paper provides an overview of these authentication mechanisms, highlighting the current state in the marketplace and describing the key enabling technologies. We conducted a qualitative analysis to identify the key factors facilitating and inhibiting the adoption of SSO and MFA by organisations using the Technology-Organisation-Environment (TOE) framework. The resulting analysis indicates a range of technologies, protocols and configurations that can be employed depending on the type of authentication and level of security required. The findings suggest that a number of technology, organisation and environment factors both positively and negatively affect organisational adoption of SSO and MFA.*

- Research and Markets: Global Multi-Factor Authentication Market 2011-2015

> *TechNavio's analysts forecast the Global Multi-factor Authentication market to grow at a CAGR of 21.3 percent over the period 2011-2015. One of the key factors contributing to this market growth is the rising number of regulatory requirements. The Global Multi-factor Authentication market has also been witnessing the increasing popularity of phone-based authentication solutions. However, the increasing total cost of ownership could pose a challenge to the growth of this market.*
>
> *This report has been prepared based on an in-depth analysis of the market with inputs from industry experts. The report covers the Americas, EMEA and APAC regions; it also covers the Global Multi-factor Authentication market industry landscape and its growth prospects in the coming years. The report also includes a discussion of the key vendors operating in this market.*
>
> *According to the report, the growing need to comply with regulations as set by various governments is one of the major drivers for the Global Multi-factor Authentication market. Enterprises are required to comply with these regulations and standards in order to secure their data. In cases of non-compliance, these enterprises may have to pay penalties that could damage their reputation. Thus, stringent regulatory norms are one of the major drivers for this market.*

- Gartner Magic Quadrant for User Authentication

> *Enterprise interest in OTP methods, broadly defined, remains high; however, as has already been noted, we have seen a significant shift in preference from traditional hardware tokens to phone-based authentication methods. Wide-focus user authentication vendors offer all these and more, generally offering or supporting knowledge-based authentication (KBA) methods or X.509 tokens (such as smart cards) as well. Most of the tight-focus vendors offer just phone-based authentication methods, especially OOB authentication methods (sometimes incorporating voice recognition as an option), with a few (none of which are included in this Magic Quadrant) offering only KBA or biometric authentication methods.*
>
> *A number of the vendors included in this Magic Quadrant have WFD tools (see "Magic Quadrant for Web Fraud Detection") that are primarily aimed at financial services providers but have attracted interest from enterprises in other sectors, notably government and healthcare. WFD tools provide adaptive access control capabilities; several vendors use the term "risk-based authentication," but the scope of these solutions goes beyond authentication alone (see "Adaptive Access Control Emerges").*
> *Adaptive access control uses a dynamic risk assessment based on a range of user and asset attributes, and other contextual information — for example, transaction value, endpoint identity and status, IP reputation, IP- or GPS-based*

> *geolocation, and user history and behavior — to make an access decision. Above a defined risk threshold, the tool can be set to deny a transaction, allow it but alert, prompt for reauthentication or authentication with a higher-assurance method, prompt for transaction verification, and so on. This capability provides an essential component in a layered fraud prevention approach (see "The Five Layers of Fraud Prevention and Using Them to Beat Malware").*
> *In typical enterprise use cases, adaptive access control capability can minimize the burden of higher- assurance authentication on the user by limiting its use to those instances where the level of risk demands it. For example, if a user accesses a VPN or Web application from a known endpoint and location, then a legacy password alone may suffice; however, if the endpoint is unknown or the location is unusual, then the user would, for example, be prompted to use OOB authentication. Gartner projects that, during the next two to three years, such capability will become more important over a wider range of use cases and will be more widely supported among mainstream user authentication products and services, especially among wide-focus vendors. By 2015, 30% of business to business (B2B) and business to enterprise (B2E) enterprise user authentication implementations will incorporate adaptive access control capability, up from less than 5% today.*

- Influences on the Adoption of Multifactor Authentication (2011)

> *Passwords are presently the primary method by which users authenticate themselves to computer systems. But passwords are proving less and less capable of protecting systems from abuse. Multifactor authentication (MFA) — which combines something you know (e.g., a PIN), something you have (e.g., a token), and/or something you are (e.g., a fingerprint) — is increasingly being required. This report investigates why organizations choose to adopt or not adopt MFA — and where they choose to use it. The authors reviewed the academic literature and articles in the trade press and conducted structured conversations with selected organizations that use or have contemplated using MFA. They found that the type of organization — for example, defense contractor, bank, hospital — affected its MFA choices. MFA is mandated for U.S. government agencies, which tend to use PINs and tokens for remote access. Among private users of MFA, tokens that generate one-time passwords, rather than biometrics, predominate. The researchers recommend that the U.S. government develop methodologies by which the costs and benefits of mandating MFA can be evaluated. Guidance by the National Institute of Standards to government agencies may be useful in helping them sort out the various arguments for and against mandating MFA in a given sector.*

- Proof Of Identity: How To Choose Multifactor Authentication (2010)

> *There are three key factors to consider when choosing the right solution: time, risk and cost. If you know what your users will bear in terms of time to log on, and if you can weigh the risks associated with each method against its costs, you will find the solution that fits best for your applications.*
> *User names and passwords are no longer sufficient authentication. In a time when so much business depends on the Internet, security requirements and regulatory mandates are putting pressure on business to adopt strong, multifactor authentication methods. In this Tech Center report, we explain how to weigh cost vs. risk to select the Web authentication method for your high-risk applications.*

- Tech Insight: Tips For Implementing Two-Factor Authentication (2011)

> *Two-factor authentication options have increased, and with each come benefits and problems. Picking the right one is a process of understanding the organization's need, risks, and support capabilities. Once these items are well-understood, the organization can compare solutions and choose the one that works best for its situation. Scope and implementation details are important to ensure a properly working and secure installation.*