

Click to verify





























Generate and store private keys on-board highly secure smart card-based authenticatorsGet in Touch SafeNet Authentication Client - is a middleware client that manages Thales' extensive SafeNet portfolio of certificate-based authenticators, including eTokens, SafeNet IDPrime smart cards, SafeNet IDPrime Virtual and combined PKI/FIDO devices. Offering full backward compatibility and incorporating features from previous middleware versions, SafeNet Authentication Client ensures complete support for all the above mentioned devices.SafeNet Authentication Client links applications to Thales' PKI authenticators, providing full local administration and support for multiple advanced security applications such as pre-boot authentication via partners, digital signing and disk encryption. SafeNet Authentication Client generates and stores private keys on-board highly secure smart card-based authenticators, allowing users to securely carry all their digital credentials wherever they go.Leverage your PKI Solution for multiple Use Cases SafeNet Authentication Client is available for Windows, Mac, and Linux, so your organization can take full advantage of SafeNet's solutions ranging from identity and access management, certificate based security, strong authentication, encryption and digital signing, from virtually any device. Find out how to secure your organization across all platforms using a fully customized, single certificate-based authenticator with SafeNet Authentication Client. Contact a specialist about SafeNet Authentication Client This brochure showcases the Thales OneWelcome PKI/CBA and FIDO Authenticator portfolio, featuring certificate-based smart cards and virtual smart card, certificate-based USB tokens, offering strong multi-factor authentication enabling organizations to address their PKI. Windows Security Antivirus SafeNet Authentication Client Manage your devices and protect the data License: Shareware Total downloads:49,829 (292 last week)Operating system:Windows XP/XP Professional/Vista/7/8/10/11Latest version:10.8.2154 Report incorrect info Enable the operation of USB keys and eToken smart cards, as well as iKey tokens as part of the operating systems supported by the SAC. Protect your data by using two-factor authentication for the network, manage your devices, customize the client and tweak the security parameters. You can download SafeNet Authentication Client 10.8.2154 from our software library for free, SafeNet Authentication Client relates to Security Tools. The actual developer of the software is SafeNet, Inc. The latest installation package occupies 13.5 MB on disk. The following versions: 10.7, 8.3 and 8.2 are the most frequently downloaded ones by the program users. This download was checked by our antivirus and was rated as safe. The latest version of the program can be installed on PCs running Windows XP/XP Professional/Vista/7/8/10/11, both 32 and 64-bit. The program's installer files are commonly found as SACMonitor.exe, Client.exe or SACTools.exe etc. From the developer: SafeNet Authentication Client is a unified middleware client that manages Thales's SafeNet portfolio of Identity and Access Management Solutions, including certificate-based authenticators such as eToken, IDPrime smart cards, and USB and software-based devices. You may want to check out more software, such as O&K Authentication Client, WatchGuard Authentication Client or SafeNet MobilePASS, which might be related to SafeNet Authentication Client. Latest update: Jan 27, 2025 Provide simple, secure access to all your apps with authentication everywhere SafeNet Trusted Access is an access management and authentication service that ensures no user is a target by allowing you to expand authentication to all users and apps with diverse authentication capabilities. Because it gives you the power to control access to all apps with the right policy, you can enforce the right authentication method for the right user. Simplify user access to cloud services and enterprise apps, streamline cloud identity management, and eliminate password hassles for IT and users with SafeNet Trusted Access, while getting a single pane view of access events across your app estate to ensure that the right user has access to the right application at the right level of trust. Video from Thales Cloud Protection & Licensing Thales's SafeNet Trusted Access is an access management and authentication service. It ensures no user is a target by allowing you to expand authentication to all users and apps with diverse authentication capabilities. And it gives you the power to control access to all apps with the right policy that enforces the right authentication method for the right user, in the current circumstances. Ensure no user is a target SafeNet Trusted Access is unique in its ability to meet the diverse needs of diverse users in your organization. Every user is a target. But not every user is the same. Some users might be logging onto secure systems in a mobile-free operational environment while others may be accessing an HR platform that contains sensitive information. Taking a one-size-fits all approach to authentication is liable to lead to security vulnerabilities. With its broad and powerful authentication capabilities, SafeNet Trusted Access meets the specific needs of diverse users by offering the right authentication method for the right user. Offering contextual/adaptive and modern authentication capabilities, through high-assurance FIDO devices, as well as Push and pattern-based authentication, SafeNet Trusted Access allows you to expand secure access to any app and all users, by enabling users to authenticate anywhere, whatever their circumstances. Integrates with your environment SafeNet Trusted Access fits into IT environments smoothly and flexibly. Delivered in full SaaS or hybrid mode, it offers the benefits of modern, policy-based access with security by design. Automated workflows and user-initiated enrollment ensure remote support for thousands of users wherever they are, while diverse integration methods ensure you can protect any application - in the cloud, or on-premises. Core CapabilitiesBenefits Powerful authentication capabilities SafeNet Trusted Access offers powerful and expansive modern authentication capabilities that meet the needs of diverse users and user types. Broad integration methods Protect a broad range of applications with diverse technologies including: SAML, OIDC, WS Fed, cloud-based RADIUS, agents, REST and SCIM APIs and an application gateway. Smart Single-Sign-On Conditional access ensures users only have to re-authenticate when their access context is risky. Risk scoring and policy configuration Powerful policy configuration, risk scoring and end-device risk assessments ensure you enforce the right access policies for the right apps and users, and maintain the integrity of all authentications. Data-driven Insights A full audit trail of access events as well as automated log export and seamless integration with SIEM systems ensure continuous monitoring and compliance. Flexand delivery architecture Implementation is available in full SaaS delivery or hybrid mode. SafeNet Trusted Access allows your organization to thrive by providing secure access to all your apps, with authentication everywhere. Expand authentication to more users With its powerful authentication capabilities, you can expand authentication to more users by meeting specific authentication needs. Apply authentication to more apps Flexible integration technologies ensure you can protect all apps and users including: cloud services, web apps, non-standard apps, on-premises resources, desktops. Deploy quickly and smoothly Automated user provisioning and workflows, full SaaS delivery, and user initiated authentication enrollment ensure speedy remote implementation for thousands of users. Complement existing solutions Complement access security and IDPs already deployed with additional authentication capabilities and expand secure access to more users and user types. Offer user convenience with passwordless authentication Ensure broad user adoption, reduce helpdesk calls and enhance security by deploying a range of passwordless options including FIDO, Windows Hello and other passwordless methods. ImageTitleLinkProduct Brief: SafeNet Trusted Access DOWNLOAD THE OLDER VERSION BELOW: Windows: SafeNet Authentication Client v10.9 GA (32-Bit and 64-Bit) SafeNet Authentication Client v10.8 R6 (32-Bit) SafeNet Authentication Client v10.8 R6 (64-Bit) Supports: Windows 11 Windows 10 Windows Server 2022 Windows Server 2019 Windows Server 2016 Windows Server 2012 R2 SafeNet Authentication Client v10.6 GA (32-Bit) SafeNet Authentication Client v10.6 GA (64-Bit) Supports: Windows 10 - Up to Redstone 5 (1809) Windows Server 2016 Windows Server 2012 / 2012 R2 MacOS: SafeNet Authentication Client v10.8 R2 GA Supports: MacOS Sonoma MacOS Ventura MacOS Monterey SafeNet Authentication Client v10.8.29.0 Supports: MacOS Big Sur MacOS Catalina SafeNet Authentication Client v10.8.28.0 Supports: MacOS Mojave MacOS High Sierra SafeNet Authentication Client v10.0.26.0 Supports: MacOS Sierra MacOS El Capitan SafeNet Authentication Client v9.1.10.0 Supports: MacOS Yosemite MacOS Mavericks Linux: SafeNet Authentication Client v10.8 R1 GA Supports: CentOS 8 / 9 Fedora 34 / 36 / 37 Red Hat 8 / 9 Ubuntu 20.04 / 22.04 SafeNet Authentication Client v10.8.28 GA Supports: CentOS 8.3 Fedora 34 RedHat 8.3 Ubuntu 20.04 SafeNet Authentication Client v10.7 GA Supports: CentOS 6.10 / 7.6 Debian 9 Fedora 30 RedHat 7.6 / 8 SUSE 15 Ubuntu 18.04.2 LTS / 19.04 SafeNet Authentication Client v10.0 Post GA Supports: CentOS 6.9 / 7.3 Debian 9.0 Fedora 26 RedHat 6.9 / 7.3 SUSE 12.2 Ubuntu 16.01 / 17.04 SafeNet Trusted Access is an access management and authentication service that enables quick deployment of multiple authentication journeys to expand your MFA coverage, allowing you to reduce insider and outsider threats.Because it gives you the power to control access to all apps with the right policy, you can enforce the right authentication method for the right user.With SafeNet Trusted Access, you can simplify user access to cloud services and enterprise apps, streamline cloud identity management, and eliminate password hassles for IT and users. You can also get a single-pane view of access events across your app estate to ensure that the right user can access the right application at the right level of trust. of surveyed IT organizations said they had a good experience using SafeNet Trusted Access of surveyed IT organizations said it was easy for their organization to deploy/implement STA of surveyed IT organizations said they benefit from the multiple authentication methods that STA provides (Source : TechValidate Survey 2022) SafeNet Trusted Access is unique in its ability to meet the diverse needs of diverse users in your organization, by proposing the right authentication method for the right user.Practices or concept that may have worked for us in the past, are no longer valid for the reality today. Every user is a target, there is no longer a clearly defined perimeter to defend. At the same time not all authentication methods are created equal and can fit all use cases and users in your organization. That is why it is no longer relevant to assume that the authentication and access management solution you have can necessarily protect you in the future. Until now you might have checked a box in implementing MFA for your IT staff but as we've in these examples, attacks focus on all types of users. Relying on what used to work for you in the past is liable to lead to blind spots in an organization's security assumptions. At Thales we believe that organizations can manage their digital transformations securely by providing more apps and more users through better MFA coverage. In today's threat environment all users and applications are targets. That's why to ensure anywhere secure access, MFA should be expanded to cover all potential targets.Offering contextual/adaptive and modern authentication capabilities, through high-assurance FIDO devices, as well as Push and pattern based authentication, SafeNet Trusted Access allows you to expand secure access to any app and all users, by enabling users to authenticate anywhere, whatever their circumstances. Smart Single Sign-On lets users log in to all their cloud applications with a single identity, eliminating password fatigue, frustration, password resets and downtime. SafeNet Trusted Access processes a user's login requests and ensures that SSO is applied intelligently, based on previous authentications in the same SSO session and the specific policy requirements applicable to each access attempt. In this way, users may authenticate just once in order to access all their cloud applications, or provide additional authentication as configured in the policy. SafeNet Trusted Access supports numerous authentication methods and allows you to leverage authentication schemes already deployed in your organization. The broadest range of authentication methods and form factors supported combined with context-based authentication enhances user convenience and allows you to manage risk by elevating trust only when needed. SafeNet Trusted Access offers flexible access management through a simple to use policy engine that gives customers real-time control over the ability to enforce policies at the individual user, group or application level. The policy engine supports a broad range of authentication methods, including ones already deployed, allowing organizations to leverage their current investments and use them to secure cloud and web-based services. As a cloud-based service, SafeNet Trusted Access can be deployed rapidly and can scale easily to meet your organizations evolving needs. Easily add hundreds of users or differentiate user groups across countries to apply regional compliance controls. In addition, with SafeNet Trusted Access offers a wide range of authentication types bundled with the service at no additional cost. Expand authentication to more users by meeting specific authentication needsApply authentication to more apps thanks to flexible integration technologiesDeploy quickly and smoothly and ensure remote implementation for thousands of usersComplement existing solutions and expand secure access to more users and user types.Offer user convenience with passwordless authentication for enhanced security and reduced costs Check out this product review of SafeNet Trusted Access. Learn how STA offers a compelling blend of security solutions that bridge the MFA, SSO and access management worlds in a single, well-integrated package. Discover how your business can bring security to access management. "SafeNet Trusted Access is an industry leading IAM solution, from a highly trusted brand, with functionality built up over more than three decades in the authentication space." SafeNet Trusted Access fits into organizational IT environments smoothly. With no infrastructure needed, and delivered as SaaS, it can be deployed rapidly and flexibly. As some of the most technically advanced and efficient organizations in the world, cloud-first companies have set a new standard for modern workforces. While global workforces require continuous access to cloud-based applications and services , it has also introduced a challenge for security teams to protect their most sensitive data and applications. Additionally, with the common misconception that secure access means heavy user friction, it makes it difficult for security professionals to get buy-in to implement a new approach to workforce authentication. Cloud-native businesses shouldn't have to compromise. With the right solution, you can protect access to applications and data without disruptions—delivering frictionless user experience while upholding the security standards you've committed to as an organization. Contact a specialist about SafeNet Trusted Access IAM leaders should seek toolsets that minimize account takeover risks and optimize user experience as part of a cohesive cybersecurity strategy that reflects human-centric design. Download the 2025 Gartner® Market Guide for User Authentication and explore how MFA, FIDO protocols, and identity-first security optimize user experience and reduces risks. Gartner has recognized Thales as a Visionary in the "Magic Quadrant for Access Management, December 2024." "Workforce access management capabilities are mature, but innovation is slowing. CIAM product features are thriving, machine IAM capabilities are increasing and partner IAM capabilities are in demand." Explore the Passwordless Authentication Leadership Compass where KuppingerCole identifies the leaders in the market and presents you with a compass to help you to find the product or service that best meets your needs. In this report, IDC studied global providers of advanced authentication services and surveyed customers that are using these technologies. Learn more about the authentication market and why Thales was named a Leader in advanced authentication. Read this KuppingerCole Executive View report on why Thales SafeNet Trusted Access Platform is a market leading Enterprise Authentication and access management solution that is highly scalable and built for environments that require the highest security levels and offers a variety of hard and soft token solutions as well as FIDO compliant authenticators. An overview of the emerging authentication landscape and the challenges towards a modern, dynamic access security. Examines how supporting a range of user authentication journeys can help organizations balance strong security with a smooth user experience. Cloud-based applications play a vital role in fulfilling productivity, operational and infrastructure needs in the enterprise. The burden of managing users' multiple cloud identities grows as more cloud apps are used. Explore the Enterprise Authentication Leadership Compass where KuppingerCole identifies the leaders in the authentication solutions market. Organizations are on a cloud migration journey. Many have implemented various on-premises Microsoft solutions, such as Office suite and AD FS, are migrating - primarily Office 365 - into the cloud. SafeNet can help protect your Microsoft cloud-based services and scale it securely in the cloud. Access this white paper to understand how NIST's recommendations and guidelines for implementing Zero Trust security can help you secure apps and data in your organization. Digital transformation, the proliferation of disruptive technologies and emerging trends such as 'work from home', coupled with the alarming increase in data breaches and security incidents have rendered the concept of trust extinct. Zero Trust security is based on the tenet "Never Trust, Always Verify," views trust as a vulnerability, and requires strict and continuous identity verification to minimize implicit trust zones. Securing and managing cloud identities is central to an enterprise's IAM strategy. Enables organizations to easily apply multi-factor authentication to secure access to any application, from any device, anywhere. SAML based Authentication is a method of identity verification that leverages an identity provider to authenticate users centrally to a broad range of unaffiliated websites. Offers easy access to cloud applications. Learn how you can have access to all cloud apps with just a single identity today! Learn more about our market-leading solutions Get in contact with a SafeNet Trusted Access specialist Contact Us The SafeNet Authentication Client is a tool which allows you to access a SafeNet USB hardware token and Code Signing or Document Signing certificate. The client includes the drivers for the SafeNet USB token as well as a client which is used to install and manage certificates. When you sign a file, the client will prompt you for a password, ensuring that only authorised members of your team can access the certificate stored on the token. Download a copy of the SafeNet Authentication client here. Note: This link includes the Windows, MacOS and Linux versions of the client. Installing the SafeNet Authentication client: Run the SafeNet Authentication Client installer. In the SafeNet Authentication Client Setup Wizard, complete the following steps to install the drivers: On the Welcome to the SafeNet Authentication Client Installation Wizard page, click Next to begin the software installation process. On the Interface Language page, in the drop-down list, pick a language for the interface and then click Next. On the License Agreement page, read through the license agreement, select I accept the license agreement and then click Next. On the Destination Folder page, choose where you wish to install the SafeNet Authentication Client and then click Next. On the Setup Type page, select Typical for the installation type and then click Next. On the Wizard is ready to begin installation page, click Install. It may take a few minutes to install the software. On the SafeNet Authentication Client has been successfully installed page, click Finish to exit SafeNet Authentication Client Setup. You have successfully installed the SafeNet Client Software. Safenet is a risk management service provider established in 1995. The company is owned privately and believes that long-term success is achieved by delivering consistent value for money to our valued clients. Safenet North America LLC and Safenet Security Services (Pty) Ltd is a global provider of high-risk security services, training, construction, life support and logistic solutions. Read More Integrated Security Solutions Critical Infrastructure Protection Facility Protection Security Intelligence Demining Life Support Services Medical Services Procurement of Services and Equipment Air Support Services Training Construction Read More World-class Management Total commitment and integrity Responsive to an ever-changing environment Work to predefined budget & timeline Recent experience in conflict zones Team integration of local staff via comprehensive skills transfer process Read More Civil engineering & construction organizations Government & international organizations - DOD/DOS/Armed Forces Oil & gas industry Transport and Logistics suppliers (Air, land, sea) Mining Sector Energy and Power Read More Safenet enables governments, non-governmental, international and commercial clients to achieve their operational goals and objectives across the globe. The company offers an array of services and solutions to support critical infrastructure protection, conflict and post-conflict reconstruction, humanitarian work and emerging market requirements. Safenet operates across the world with principal offices in UAE, Afghanistan, South and East Africa as well as in Georgia, USA. In providing strategic consultancy to protecting individuals and assets, developing complex security and crisis management plans and PSD training, Safenet has established a value chain of products and services that have secured a diverse and impressive range of clients.Read More SafeNet Trusted Access © Copyright 2019-2025, Thales Group +1 410-469-1651 supportportal.thalesgroup.com Information security company Not to be confused with SafeToNet or SafenNet. SafeNet, Inc. Company typesSubsidiaryIndustryInformation securityFounded1983; 42 years ago (1983), in Timonium, Maryland, United StatesArea servedWorldwideProductsEncryption, Semiconductor IP, software monetization, Software as a Service, hardware security modules, authentication, security tokensNumber of employees1,600 (2011)ParentThales GroupDivisionsData Protection, Software MonetizationWebsitecpl.thalesgroup.com SafeNet, Inc. was an information security company based in Belcamp, Maryland, United States, which was acquired in August 2014 by the French security company Gemalto was, in turn, acquired by Thales Group in 2019. The former SafeNet's products include solutions for enterprise authentication, data encryption, and key management. SafeNet's software monetization products are sold under the Thales Sentinel brand. SafeNet was notably one of the largest suppliers of encryption technology to the United States Government.[1] On 8 August 2014, Gemalto announced that it had signed a definitive agreement to acquire 100% of the share capital of SafeNet from Vector Capital for US\$890 million on a debt free/cash free basis.[2] A subsequent acquisition of Gemalto by French rival Thales Group was completed on 2 April 2019.[3] This section needs additional citations for verification. Please help improve this article by adding citations to reliable sources in this section. Unsourced material may be challenged and removed. (May 2024) (Learn how and when to remove this message) 1983: SafeNet, Inc is founded in 1983 in Timonium, MD as Industrial Resource Engineering by two former NSA engineers, Alan Hastings and Douglas Kozlay. 1986: Anthony A. Caputo becomes a silent investor in the company. 1987: Anthony Caputo takes the helm of the company as CEO and changes the name to Information Resource Engineering. 1988: Lawrence Livermore Labs becomes IRE's first major customer. The company moves its operations to White Marsh, MD. 1989: IRE goes public in an IPO initially trading on the OTC pink sheets. 1989: IRE rapidly becomes the leader in banking communications security with seven of the top ten U.S. banks as customers and encryption devices used by SWIFT (global interbank transfer system). An end-to-end encryption system was developed that secured data over an X.25 public network, providing the world's first "virtual private network." Early adopters included the Bank of Montreal and Citibank. 1994: IRE acquires Connective Strategies, Inc., a manufacturer of voice and data ISDN products founded by its CEO, Charles Brown. October 1995: IRE acquires Swiss crypto manufacturer Gretag Data Systems for \$4 million. 1996: MCI Communications launches the first commercial VPN service using SafeNet VPN technology developed by Charles Brown of SafeNet and Vinton Cerf of MCI. SafeNet is adopted by thirteen of the top fifteen U.S. banks within two years. 1997: IRE stock plunges 50% in one day on the announcement of the restructuring of the MCI contract. July 1998: Major shareholder fails in a hostile takeover attempt of IRE.[4] 2000: IRE is renamed SafeNet, Inc. after the VPN product line. 2001: Company co-founder Doug Kozlay leaves SafeNet to form Biometric Associates, a technology company focused on biometric-based authentication and identity solutions. 2002: SafeNet acquires a Dutch company Securealink. With the collapse of the tech "bubble," SafeNet, as a public company with a strong sales channel[citation needed], was able to acquire a series of promising security companies at deep discounts. February 2003: SafeNet acquires Cylink and Raqia Networks[5] October 2003: SafeNet acquires the OEM business of SSH Communications Security[6] November 2003: SafeNet moves its corporate offices to Belcamp, MD. March 2004: SafeNet acquires Rainbow Technologies.[7] December 2004: SafeNet acquires Datakey, Inc April 2005: SafeNet acquires DMDSecure B.V.[8] June 2005: SafeNet acquires MediaSentry December 2005: SafeNet acquires Eracom Technologies AG[9] 2006: SafeNet was involved in the options backdating controversy. As a result, both the chief executive officer and the chief financial officer resigned, and in 2008 the company's former CFO was sentenced to six months in prison for manipulating employee stock options.[10][11][12] April 2007: California-based financial company Vector Capital buys Safenet for \$634 million, making it private[13] April 2008: SafeNet acquires Ingrian Networks, Inc. May 2008: SafeNet acquires Beep Science AS March 2009: SafeNet parent company, Vector Capital acquires Aladdin Knowledge Systems[14] April 2009: SafeNet sells MediaSentry to ArtistDirect December 2009: SafeNet acquires Assured Decisions, LLC[15] December 2012: SafeNet sells its Government Solutions business unit to Raytheon[16] August 2014: SafeNet announces it is to be acquired by Gemalto by the 4Q of 2014[17] February 2015: SafeNet Assured Technologies is launched as a fully owned subsidiary of Gemalto to provide high-assurance data security products and technologies to the U.S. Government.[18] April 2019: Thales Group closes the acquisition of Gemalto.[19] Thales Cloud Protection and Licensing were formed to serve the global community, and SafeNet Assured Technologies, the entity serving the U.S. Government, becomes Thales Trusted Cyber Technologies. The former Rainbow Technologies subsidiary SafeNet Government Solutions, formerly SafeNet Mykotronx, is still based in Torrance, California with offices in Irvine, California and Columbia, Maryland.[20] The company was founded in 1979 as Myko Enterprises. It changed its name to Mykotronx, Inc in 1987 and merged with SafeNet as part of the SafeNet merger with Rainbow in 2004.[21] SafeNet Government Solutions, LLC has been operationally merged into SafeNet and the lines between the two organizations have been intentionally blurred due to financial reasons. SafeNet Government Solutions is no longer considered a subsidiary. SafeNet Government Solutions provides information security and communications security technology for the US government. The firm has an indefinite-delivery, indefinite-quantity contract for its KIV-7 line of commercial off-the-shelf cryptographic devices that provide protection for digital and voice communications through TOP SECRET, used by agencies such as the National Security Agency (NSA) and the National Reconnaissance Office.[22] Other products include the KOV-14 Fortezza Plus PC card which was developed as part of the NSA's NSSI program and is used on Secure Terminal Equipment.[23] They previously developed the Clipper chip.[24][25] In 2009, Vector Capital acquires Aladdin Knowledge Systems, and placed it under SafeNet with the annotation of "under common management". In 2010, the two companies were officially merged. ^ Roseanne Gerin (2005-04-10). "SafeNet wins DOD network security deal". Washington Technology Magazine. Retrieved 2008-12-08. ^ "Gemalto to acquire SafeNet, the worldwide leader in data and software protection". 2014-08-08. Retrieved 2014-08-13. ^ "Thales Completes Acquisition of Gemalto to Become a Global Leader in Digital Identity and Security, Extending U.S. Footprint" (Press release). ^ "Coup fails". 11 July 1998. ^ EETimes (2003-02-28). "EETimes - SafeNet acquires assets of Raqia Networks ". EETimes. Retrieved 2020-09-17. ^ "SSH sells its OEM business to SafeNet". 2003-10-14. Archived from the original on 2006-11-28. Retrieved 2008-12-03. ^ "SafeNet, Inc. Announces Close of Merger with Rainbow Technologies". 2004-03-14. ^ EETimes (2005-03-25). "EETimes - SafeNet to acquire software provider "- EETimes. Retrieved 2020-09-17. ^ GmbH, finanzen net. "SafeNet Completes Acquisition of Eracom Technologies AG | Markets Insider". markets.businessinsider.com. Retrieved 2020-09-17. ^ Jones/Associated, Dow (October 19, 2006). "SafeNet Is Rolled by Options Inquiry". The New York Times. Retrieved 2013-11-21. ^ Graybow, Martha (28 January 2008). "Ex-Safenet CFO gets prison term in options case". Reuters.com. ^ "Cost of Backdating: Six Months, \$1 Million". 2008-01-30. Retrieved 2013-11-21. ^ "SafeNet sold, goes private". 2007-04-13. ^ "Aladdin Knowledge Systems Completes Merger with Vector Capital Affiliate" (PDF). 2009-03-24. Archived from the original (PDF) on 2009-04-19. Retrieved 2010-06-02. ^ "SafeNet to Acquire Assured Decisions, LLC". Bloomberg News. 2009-12-23. ^ "Raytheon Acquires SafeNet Inc". finance.yahoo.com. 13 December 2012. Retrieved 2020-09-17. ^ "Gemalto Buys SafeNet for \$890 Million". WSJ.com. 2014-08-08. Retrieved 2015-01-09. ^ "SafeNet Assured Technologies, LLC Formally Launches U.S. Based Business". 2015-02-09. ^ "Thales buys Gemalto". 2019-04-02. ^ "SafeNet Offices - North America". ^ "About SafeNet Mykotronx". ^ "KIV-7 Family". Federation of American Scientists. ^ "Mykotronx wins defense card work". ^ "INFORMATION ABOUT THE CLIPPER WIRETAP CHIP". ^ Neumann, Peter G. (21 April 1993). "THE CLIPPER CHIP: A TECHNICAL SUMMARY". The Risks Digest. 14 (52). Official website U.S. Subsidiary Website Retrieved from "