Klōke, LLC Intellectual Property

Issued Patents

KLŌKE
7,937,579 System, method and apparatus for electronically protecting data and digital content

This first family secures data. The need for better security became apparent in 2005 with the ChoicePoint data breach when a firm was set up to purchase data for the sole purpose of stealing identities. Traditional cybersecurity had failed and it was clear that future threats would make things much worse. Its design requirements included:

- All data security at the time was based on math, so as computers got faster, the math had to become more complex to remain safe. Moore's Law would one day be obliterated by quantum computers being developed by U.S. adversaries, particularly China. **Solution:** withstand an attacker with infinite computing power.
- The second level of security ensures that secured data cannot be reverse-engineered. **Solution:** ensure that protected data has no owner or source.
- The third level of security protects against bypassing authentication. **Solution:** the retrieval instructions are stored with authentication.
- Security must meet current and future configuration needs. **Solution:** security is device, app, network, location, and data type agnostic.
- Attack surfaces would increase and perimeter defenses would fail. **Solution:** protected data cannot be reverse-engineered.
- Rather than degrade, security must get stronger over time without having to change applications. **Solution:** authentication upgrades are centrally controlled and retroactively applied.
- Improve retroactive privacy compliance and special needs processing: **Solution:** pre and post-processing plug-ins examine process all requests.
- Improve data usage and visibility. **Solution:** real-time threat intelligence is baked-in for authentication, plug-ins, and data request.
- Generate data for improved IA and machine learning needs. **Solution:** all threat intelligence is automatically logged.

Our research found a proven design from World War II in the way in which the massive cathedral stained glass windows were protected from theft. Individual pieces of glass were given randomly to parishioners who were told to hide them. As a result, no single person knew where the art was stored. For Klōke, the data is secure with no context while the original file (like a lead frame) is the context with no asset.

This was the basis for 7,937,579. Patents require illustrative examples to describe the invention, so the term "pointers" was used as in random data in a file "pointing" to unknown secure vaults. Seven months after the provisional application was filed, the PCI industry introduced the term "tokens" to protect payment data. As such, 7,937,579's inventor is considered the first-to-invent token data security.

Continuations were filed for 8,543,806, 8,261,058, and 8,826,448, and the term "pointers" is references more than a thousand times.

7,937,579 retroactive capabilities means that evolving threats such as SolarWinds and quantum computers are within the design objectives.

The strongest patents are the ones that have been successfully litigated in court. The second strongest are the ones that have been accepted and cited by recognized firms. The following 7,937,579 citations are as of 9/1/2021:

Document Cited	Issued Patents Citing Peckover Reference	Owner
2006/0212698	8,356,097	Compete, Inc. (Boston, IA)
2006/0212698	8,396,788	SAP AG (Walldorf, DE)
2006/0212698	8,401,183	Verizon Patent and Licensing Inc. (Basking Ridge, NJ)
7937579	8,473,324	Bank of America Corporation (Charlotte, NC)
2006/0212698	8,522,341	SAP AG (Walldorf, DE)
2006/0212698	8,621,214	Securencrypt, LLC (Jackson, MI)
2006/0212698	8,626,834	Compete, Inc. (Boston, MA)
2006/0212698	8,751,644	SAP AG (Walldorf, DE)
2006/0212698	8,769,080	Compete, Inc. (Boston, MA)

Document Cited	Issued Patents Citing Peckover Reference	Owner
2006/0212698	8,793,756	DST Technologies, Inc. (Kansas City, MO)
2006/0212698	8,924,724	Securencrypt, LLC (Jackson, MI)
2006/0212698	8,954,580	Compete, Inc. (Boston, MA)
7937579	8,955,159	Sony Corporation (Tokyo, JP)
7937579	8,983,918	Bank of America Corporation (Charlotte, NC)
2006/0212698	9,092,788	Compete, Inc. (Boston, MA)
2006/0212698	9,104,534	Microsoft Technology Licensing, LLC (Redmond, WA)
2006/0212698	9,105,028	Compete, Inc. (Boston, MA)
2006/0212698	9,111,305	Amazon Technologies, Inc. (Reno, NV)
2006/0212698	9,112,886	VERIZON PATENT AND LICENSING INC. (Basking Ridge, NJ)
2006/0212698	9,123,056	VERIZON PATENT AND LICENSING INC. (Basking Ridge, NJ)
2006/0212698	9,129,032	Compete, Inc. (Boston, MA)
7937579	9,148,418	Shannon; Matthew Martin (Tampa, FL) Decker; Matthew James (Valrico, FL)
2006/0212698	9,152,345	International Business Machines Corporation (Armonk, NY)
2006/0212698	9,292,860	Compete, Inc. (Boston, MA)
7937579	9,367,684	RealSource, Inc. (Elgin, IL)
2006/0212698	9,396,273	UBIC, Inc. (Tokyo, JP)
7937579	9,424,582	eBay Inc. (San Jose, CA)
2006/0212698	9,501,781	comScore, Inc. (Reston, VA)
2006/0212698	9,686,242	Alcatel Lucent (Boulogne-Billancourt, FR) Alcatel-Lucent USA Inc. (Murray Hill, NJ)
2006/0212698	9,900,395	comScore, Inc. (Reston, VA)
7937579	9,921,561	Secure Cloud Systems, Inc. (Marco Island, FL)
2006/0212698	10,013,702	comScore, Inc. (Reston, VA)
2006/0212698	10,296,919	comScore, Inc. (Reston, VA)
2006/0212698	10,360,587	comScore, Inc. (Reston, VA)
7937579	10,380,374	JPMorgan Chase Bank, N.A. (New York, NY)
7937579	10,503,133	Secure Cloud Systems, Inc. (Marco Island, FL)
2006/0212698	10,748,158	Refinitiv US Organization LLC (New York, NY)
2006/0212698	10,825,029	Refinitiv US Organization LLC (New York, NY)
2006/0212698	10,931,754	Amazon Technologies, Inc. (Seattle, WA)
7937579	11,012,722	Secure Cloud Systems, Inc. (Marco Island, FL)
2006/0212698	11,037,175	Refinitiv US Organization LLC (New York, NY)

Published Applications Citing Peckover Reference	Owner
JP6424382 (B1)	ZENITH CO LTD
US2007055937 (A1)	CANCEL DAVID [US] GILLETT CHRISTOPHER C [US]
US2007260514 (A1)	MICROSOFT CORP [US]
US2009135444 (A1)	BEST STEVEN FRANCIS [US] EGGERS JR ROBERT JAMES [US] GIROUARD JANICE MARIE [US] KUMHYR DAVID BRUCE [US]
US2009144619 (A1)	BEST STEVEN FRANCIS [US] EGGERS JR ROBERT JAMES [US] GIROUARD JANICE MARIE [US] KUMHYR DAVID BRUCE [US]
US2010146294 (A1)	SNEED ANTHONY [US]
US2015101065 (A1)	BIO KEY INT INC [US]
US2020211105 (A1)	ALIBABA GROUP HOLDING LTD [KY]
WO2012082910 (A1)	AMAZON TECH INC [US]
WO2017085443 (A1)	WESSEX TECH OPTOELECTRONIC PRODUCTS LTD [GB]
WO2019150588 (A1)	ZENITH CO LTD [JP]

8,613,107 System, method and apparatus for electronically protecting data associated with RFID tags

This second family secures physical devices with digital components. Some countries have added RFID tags to passports so that personal information can be quickly machine read and processed. A YouTube video quickly appeared showing how this information could be read by a smart bomb. Imagine the chaos if such a device were to be planted in Disneyland, awaiting the arrival of multiple people of a specific demographic. The problem is that adding even weak encryption increased RFID costs by 10x.

- There was a need for better RFID security as well as ending the cost dilemma.
- If the security worked on tiny RFID tags, then it would also work on any IoT or industrial device.
- This would be needed because of the exponential growth in the use of IoT and other devices that are making perimeter defenses an impossible task.

The goal therefore became focusing on RFID security that could then be universally used. The RFID standards body was called REG (for RFID Expert Group); 7,937,579's inventor joined REG to attended its next standards meeting. The purpose was to explain how the security vs. cost dilemma could be eliminated, but the REG members (including TI and Motorola) politely tabled his proposal. During a break, he was told that there was no way REG members would permit a proposal that would reduce their product sales by 10x. So he filed a patent to create Klōke's own standard:

- Attack surfaces include tiny 1¢ RFID tags all the way up to mobile phones, IoT devices, and industrial control systems. **Solution:** all devices can have 7,937,579's benefits.
- The security vs. cost dilemma puts the entire system's integrity at risk. **Solution:** the 7,937,579 benefits do not add to device cost, software, or complexity.
- System change and attack vectors change. **Solution:** central control means that upgrades are retroactively applied without increasing device costs.

Published Applications Citing Peckover Reference	Owner

7,941,376 System and method for customer authentication of an item

This third family secures physical items. Headline: Counterfeit Drugs Kill Over 700,000 People in Africa Every Year. There are many contributing factors, including how India permits counterfeit manufacturing for export. Another problem is the near total lack of infrastructure and quality control in rural areas. The human cost is unacceptable, as is the estimated $300 billion economic cost.

- The solution must complement existing supply chain systems and work anywhere in the world with no special equipment. **Solution:** a drug can be checked by any consumer using only his or her cell phone.
- The full status of a drug can be instantly verified. **Solution:** the consumer immediately gets an "OK to Use" or "Do Not Use" message, the latter signaling that the drug is counterfeit, expired, recalled, or grey market.
- The estimated global loss from counterfeit products is $600 million/year. **Solution:** this also works with all physical products, including art, collectibles, etc.
- There are many supply chain products; the crime sometimes occurs outside their control, such as a pharmacist putting counterfeit drugs on shelves. **Solution:** this bypasses all other controls and connects the consumer directly with the manufacturer or original item creator or owner,

Two other patents (8,359,271 and 10,636,040) increase the flexibility and control of 7,941,376.

Pending Applications

Klōke has several pending applications and had never had a patent application rejected. One in particular is worth mentioning because it offers an immediate solution to a major problem that cannot be prevented – ransomware:

- Hackers will always find new ways to get inside the security perimeter to see and exfiltrate sensitive data. For this reason, ransomware is also a data breach. They may threaten to block use of the data or alternatively to release it if a ransom is not paid. **Solution:** assume that hackers have full access to data and crypto keys, but sensitive data is stored elsewhere and cannot be cracked.
- The hours or days that it takes to find and restore backup data represent the amount of time that the system is down and new data is lost. **Solution:** the restore time has been reduced to hours or seconds for hot failovers.
- Sleeper attacks are when hackers infect backup data in a way that cannot be detected. This delayed exploitation of the hack means that months of backup data are lost, which forces the target to pay the ransom. **Requirement;** the patent shows *where* this is blocked but not *how (see Trade Secrets below)*.
- Ransomware cannot be prevented and most firms are poorly prepared to manage backups, restores, breach notifications, etc. **Solution:** Third Party Risk Management provisions are included for outsourcing additional services.
- A future ransomware attack could include hackers threatening to modify data. This has already happened when hackers randomly modified the blood types of active-duty military personnel. **Solution:** sensitive data cannot be altered because hackers cannot access it.

Trade Secrets

Klōke's trade secrets are designed to:

- Protect a 17 year R&D investment.
- Render publicly available patent information incomplete to competitors.
- Ensure hackers do not fully understand how Klōke works.

Some trade secret specifics are available under NDA.

How the security switches from defense to offense to identify and track attackers

Current security products can only defend. Klōke has the ability to switch from defense to offense to track hacker chains of command, collect behavioral biometrics for a central registry to warn other licensees, etc. This is referenced in the patents but not described in detail.

Preventing 'sleeper' ransomware attacks

Hackers are developing ways to infect backups in a way that cannot be detected, even with rest restores. This trade secret explains how these attacks can be detected and blocked before any damage is done, and is a major Klōke asset.

Managing different cultural expectations of different geographic regions

This permits a licensee to set up and maintain the different environments in which Klōke will operate.

How to secure physical items as well as data

Virtually all data security problems are related to loss and the lack of control. The same problems occur in the physical world. Improving physical supply chains is complex, particularly when more than one is involved, and there are sometimes gaps. This trade secret shows a simple solution to this problem that enhances all current supply chain networks.

The different ways that data is fragmented in the vault

This describes how a single object can be fragmented in more than one thousand ways.

How this IP can also be used to protect data in transit

Quantum entanglement is the most secure type of communication, but has limitations (cost, distance, hacker shutdowns). Klōke's technology offers a less expensive, distance agnostic communication method.

How to upgrade legacy systems with minimal disruption

A major problem is the cost, risks, and stress of upgrading a stable legacy system. This trade secret describes the processes that reduce these concerns.

Dynamic algorithms that change how data is stored in the vault

This describes another layer of protection that makes Klōke's micro vaults moving targets.

How bypassing authentication renders vault data useless

This trade secret ensures that raw micro vault data cannot be reverse-engineered.

Stolen credentials

The misuse of legitimate credentials has been called "exceptionally challenging to identify." Klōke has several ways to do this in real-time.