iBank Design and System Specification (DRAFT)

M. Dudziak
Institute for Sustainable Economy and Community [1]

version 1.0 5.February.2009

INTRODUCTION

This is familiar informal at present, and later all this material can be transformed into a proper CMMI-standard format.

Summary

iBank™ is the name given to the secure information management and data haven services provided to a limited-membership, worldwide community of users who are engaged in trading of goods, services, and financial securities among each other. iBank provides transaction services, trade decision support, remote conferencing, value forecasting, full-service accounting, auditing, and financial analysis functions, full-service data haven operations, within the cyber-armored environment of distributed, dynamic, multi-layer, parallel encryption and camouflage (KERBEROS™). iBank handles many types of financial and value representations including alternatives to conventional currency-based or other monetary-based standards including gold standards. iBank runs on a technology platform employing state-of-the-art web software engineering and incorporates KERBEROS for its security management services.

Format

The system architecture, design, user interface, and security functions will be illustrated extensively by means of an example drawn upon the model of the organization (“House” or “Manor House”) and an Orbis/EcOasis type communities and their members who are and will be individuals located in all parts of the world and engaged in all sorts of trade among one another but mainly in the form of resources that are products, supplies for products, energy and fuel, or commodities including livestock, precious metals, minerals and gemstones, and life-critical sustainability resources.

The user community will be described, then several use-case models, then the main architecture, then the structure of individual modules.

Examples are given frequently in marked textboxes.

All software involved in iBank consists of source modules that are either originating within TETRADYN or ISEC, or obtained otherwise in a manner that enables clear reuse, modification, and maintenance at the source level. The source code in modules varies: C++, PHP, Java, and SQL. In addition, documents use HTML and XML.

[1] At present, it appears prudent for iBank (and everything connected thereto), created and owned by Martin Dudziak, under license to TETRADYN, LLC, to be in turn licensed to the non-profit Institute for Sustainable Economy and Community, Inc., which in turn can license all software and services to others. The benefit is in having iBank operated by a non-profit humanitarian foundation.

Users, Securities, and Transactions

User Community

The users of iBank are individuals (self-representing agents) who are acting in their own capacity or as representatives (agents; e.g., employees, attorneys) of another institution in order to conduct transactions among one another, either 1:1 or in group configurations.

A special note about *entities* such as users, agents, securities, and transactions
Any entity in the iBank process space may be unitary or complex. Unitary means: one person, one representative, one "thing" constituting a security, a transaction, a trade. Complex means: consisting of two or more in some collective fashion, but dependent upon the situation, the negotiation, the terms; thus "complex" because it cannot be stated as simple as "2" or "plural."

> Example:
> Boris is a Russian businessman who owns a polymer plastics company OOO Polymer Centre near Moscow. He also collects modern abstract art, maintains a stable of riding horses, and owns a number of jewelry stores and fashion boutiques in the Caribbean.
> Dominique is an Italian businesswoman whose company, Viva la Vida Ltd., owns and operates hotels in the Caribbean, Cote de Azul and in Dubai and Bahrain. She also organizes luxury eco expeditions for tourists who wish to travel by sailing vessel and on horseback or camel caravans trips in exotic locations in Central and South America and in the imaginary Shangri-La land of Salaam-Iraq.
> Majed is a Syrian-American businessman who is in software and biomedical products, principally as a private equity investment partner, with a number of other persons from around the world. Their business, Q-Capital, has chosen to have Majed act as the agent for all iBank-related business transactions. Q-Capital buys and sells virtually all types of NASDAQ and private shares, but also they have become active recently in land holdings in the Americas and India where there is proximity to companies (in which they own interests) that produce natural medical products in an eco-sensitive manner, in keeping with principles set down by organizations such as InBio, Oeko-Tex, and WWF.
> Boris, acting as Polymer Centre, Dominique, acting as Viva la Vida, and Majed, acting on behalf of Q-Capital, are users of the iBank.

What is an iBank transaction?

Transactions are defined as being the following four types:

- ⌘ Deposit of a security
- ⌘ Withdrawal of a security
- ⌘ Trade (exchange) of a security for another security
- ⌘ Payment (for services rendered) to the iBank institution (this payment may take several forms, including not only conventional currencies or securities but iBank securities as well)

What is an iBank security?

A security can be virtually anything that an agent wishes to bank or trade. Thus, securities can be individual entities or collective groupings of:

- ⌘ commodities such as gold, oil, wheat, corn, coal, precious or heavy metals, precious gems and minerals
- ⌘ livestock such as horses, cattle, sheep
- ⌘ real estate including buildings and contents
- ⌘ fine art works, antiques, furniture, musical instruments, numismatics and other

collectibles
- ⌘ currency, conventional securities such as stocks, bonds, futures, derivatives, options, swaps, etc.
- ⌘ equity interests in both tangible and intangible projects, intellectual property, products in the process of development, manufacture, assembly, transit or inventory, or highly speculative entities such as creative visions, dreams, conceptual designs, trainings, educations, or future experiences
- ⌘ and informational entities such as facts, reports, documented or otherwise, that are perceived by the owner to be of economic (i.e., tradable, exchangeable) value to another member of the iBank user community.

Example:
Boris deposits his painting of Picasso's, "Trois femmes" (1908) into the iBank. It has been appraised at $10M despite a 2007 Sotheby's bid of only $8.5M. (He also wants to buy a Japanese polymer producer-supplier that is up for grabs, estimating it will take approx. $50M.)

Dominique deposits eight tickets on a 2-week trip that includes a 1-week riding tour in the Guanacaste Peninsula of Costa Rica, plus a 1-week sailing trip to Coco Island, a pristine preserve in the Pacific, all air travel from the USA included. They are valued by her at $5,000 apiece.
(She also is in the market for 2 horses, a new skilled first mate, and a new Land Rover. She is thinking of selling one of her small hotels on Saba if she can get something worth approx. $5M.)

Majed and his partners want to buy land that is away from large urban centers in either USA or Argentina where there will also be food production. They would like to sell off interests in oil and gas futures and one of their biomedical companies that produces special paper that has antimicrobial "litmus-test" properties, a new venture seeking a manufacturing partner.

How are iBank transactions executed?

There are always three parties to any transaction – buyer, seller, and auditor. However, these parties may be "virtual" or "implicit" in some cases. Also, these terms do not equate with their usual connotations; there are some slight differences. Part of the reasoning for this structure pertains to the design of the information management software and how processes can be better managed and secured.

Deposits

There is always a real depositor, the security owner, and this is the "seller." There is a virtual receiver, a "buyer" - the iBank. The sale is virtual since no actual goods, including currency, EFT funds, security notes, are actually received or accepted in the manner that a conventional (commercial or investment) bank receives and takes possession of a deposit or payment. The iBank is the auditor, meaning that it reviews the transaction and maintains all required history and account data for both internal bookkeeping and external review.

Withdrawals

The reverse operation of a deposit.

Payments

A buyer and a seller both make payments to the iBank on the basis of a trade, but the terms of payment will vary according to two factors: (1) the relationship between the party (buyer or seller) and the iBank, and (2) the nature of the trade. There may also be payments for non-trade reasons, such as basic membership in the iBank trading community, but these are processed in a

special manner as a trade where the type = (admin) or (null).

Trades
Like snowflakes, each trade is unique. Unlike snowflakes, all trades are not necessarily unique.

Either a seller or a buyer may initiate a trade. Securities may be traded individually or bundled. There may be all sorts of constraints set by either the trade initiator or the trade respondent. An iBank trade is quite different from a conventional one in either the investment market or in the retail store. A trade can be completed (a) without a completion of the actual transfer of the buyer's payment to the seller or the seller's security to the buyer, at the time of the trade, and/or (b) without any definite time for completion of those transfers in the future, and/or even (c) without definite determination of the final vehicle of exchange, the actual trade-currency.

Thus, an iBank trade – which is actually very close to traditional and even ancient systems of barter - introduces some new concepts that are formalizations of the barter concept, in order to accommodate a wider variety of buyers, sellers, and objects of trade and exchange. iBank trades are dynamically valued; a member may sell fifty trucks which by GAMP (Generally Accepted Market Practices)[2] have a value of somewhere between

These are briefly itemized here.

Trade-currency
The actual object of value (which may be a combination of objects of value) that the seller receives from a trade.

Trade initiator
The buyer or seller who initiates the trade process.

Trade respondent
The other party, buyer or seller, who is approached by the trade initiator and who enters into the trade process.

GAMP (Generally Accepted Market Practices)
A method of valuation for the security that is the subject of the trade.

Information Security

A distinction is made between data, information and knowledge. Data consists of records – text, numbers, documents, pictures, spreadsheets – the "stuff" of databases. Information consists of ordered and structured data that is related to some topics. Information is data that has some form. Knowledge is information that is connected with change, with the need to change something in order to solve a problem or to create an innovative, gainful advance.

Membership

The first level of information security is through membership control. This is a function of the "House" as the primary raison d'etre for this implementation of iBank as a real, functioning service. Membership control is what provides the first level fo defense against intrusion and

[2] GAMP is a new term introduced in iBank thinking, but it is hardly "new" in real-world economics. What is some object worth today? What will it be worth tomorrow, or in a year? There are many formal methods from the investment world for estimating the value of a stock, bond, commodity, option, derivative or currency. These methods can be used by both buyer and seller, with the assistance of the iBank providing an unbiased consultant as auditor-broker of the trade,

abuse. Membership control is the Human Element, the most critical and also vulnerable aspect of any encryption system, any intelligence network, any secret. A "one-time pad" is the ultimate and only truly unbreakable, uncrackable encryption scheme. No supercomputer can break it. However, a disclosure of the one-time pad can be done by a person, and once done, all hell can break loose.

Meetings

The users of iBank conduct trades by meeting and negotiating. How does this happen? In person, on the "porch," in the office, in the gym, in the bedroom maybe, or through the internet. All of these are vulnerable in their own ways. Information security is not only about software and algorithms to control viruses, worms, and bots. It is also about physical security, microwave defense, van Eck keystroke and monitor signal-tapping, and all that good stuff.

Data Encryption

The "crypto" issues are less about keys, strings, prime numbers, and algorithms, and more about human adherence to basic principles and protocols. "Use it always, or lose it sometime, maybe, when you least expect it."

There are several channels of electronic communication where encryption is used within the iBank. Email, phone, video, file-sharing, form-filling, web access in general, and data storage.

Standard encryption applies to interactive communications and transmissions. the heart of the matter is what goes on inside the iBank as the broker, arbitrator, consultant, auditor and data manager of everything that pertains to a member's activities and holdings, including their files that represent in some cases the entirety of a security's content, and in most cases sufficient information by which someone can answer all the critical questions of who, what, where, when, and how.

KERBEROS handles the data haven operations of storage, archiving, and foremost of all, organizing, relating and correlating. KERBEROS is used to ensure that if some person X were to obtain even 100% of perfectly decrypted data on a particular buyer, seller, trade or payment, that this X will have only scanty, incomplete, noisy and misleading data, insufficient to "cause trouble" for the member or members of the iBank.

KERBEROS

The essence of KERBEROS is not any one particular encryption protocol (several are used), nor anything about the hardware or the physical locations of any server. The strength of KERBEROS rests in the way data is fragmented, mixed, divided and distributed.

The technical details of KERBEROS are described in other documents. They are sensitive trade secrets and involve a very innovative approach to "data haven" technology. Encryption is employed, but KERBEROS is not merely a new form of encryption. That would render it vulnerable to cryptanalysis techniques available to not only government agencies but private corporations, competitors, and criminals. KERBEROS is very exacting and employs multiple algorithms, multiple human-intensive steps, and in the end, it is as strong as the combination of the classic unbreakable "one-time pad" and the integrity of the persons managing and operating the iBank as an institution. Swiss banks and other institutions once enjoyed a very strong reputation because of the uncompromising integrity of the persons making up the institutions. One cannot have extremely strong data security and privacy without also having extremely strong persons, not only relying upon algorithms and computers.

