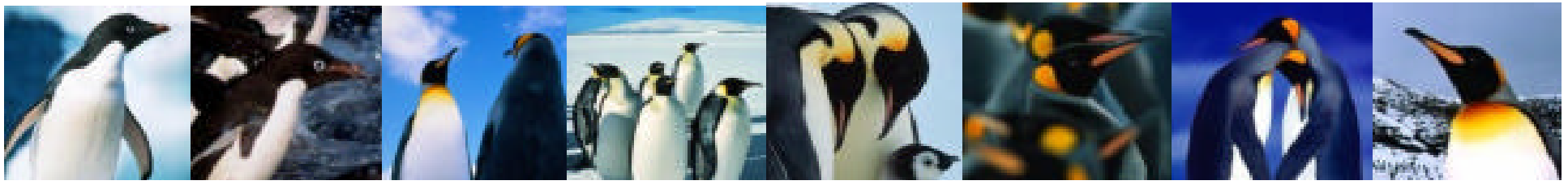
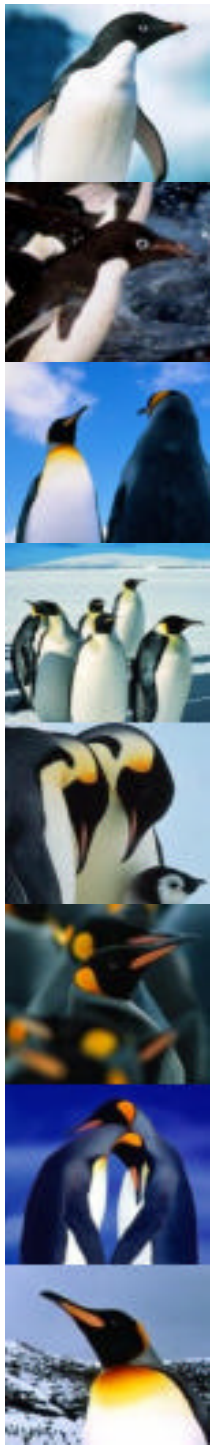
Introduction to the Manager's guide to PKI

Steve Mathews



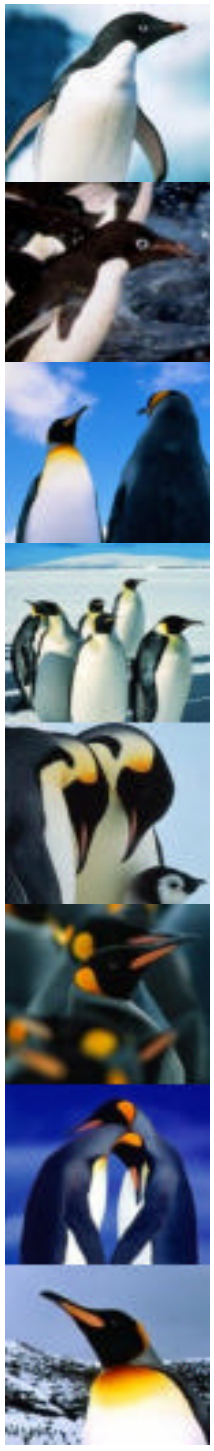


ArticSoft

Background

- The security group in Open Group has long recognized the practical difficulties faced by security professionals explaining the complexities of security (and supporting) technologies to management
- Management understanding is seen as a pre-requisite to achieving support and real implementation of security programs

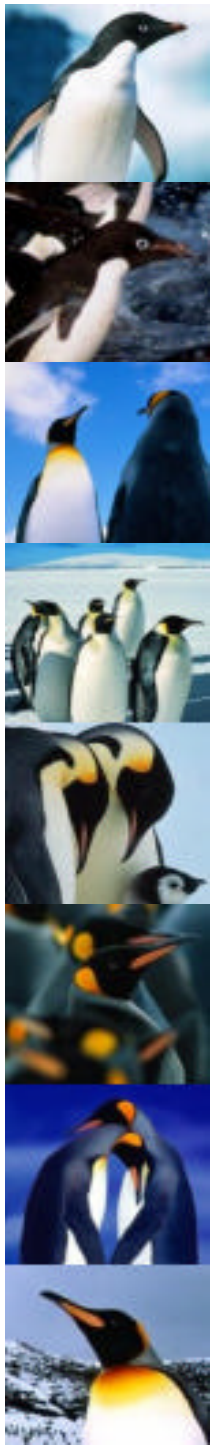
© ArticSoft Ltd 2003



Background

- Security Group have made their focus developing Management Guides that are informative and non-technical
- The focus of guides is to help managers understand what is required and how to make informed choices given alternative ways to proceed
- Guides are not prescriptive, final choices must be left to the business using the guide
- Advice offered is disinterested

© ArticSoft Ltd 2003

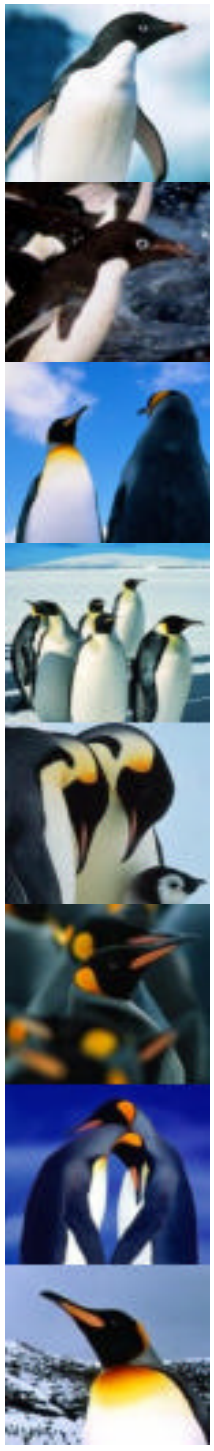


ArticSoft

Start point

- It has long been recognized by the group that public key cryptography is a critically important security technology
- However, it is also recognized that there are many issues to understand if this technology is going to be implemented successfully
- It is also recognized that the most publicized form – PKI – may not always be the most suitable method for all situations

© ArticSoft Ltd 2003

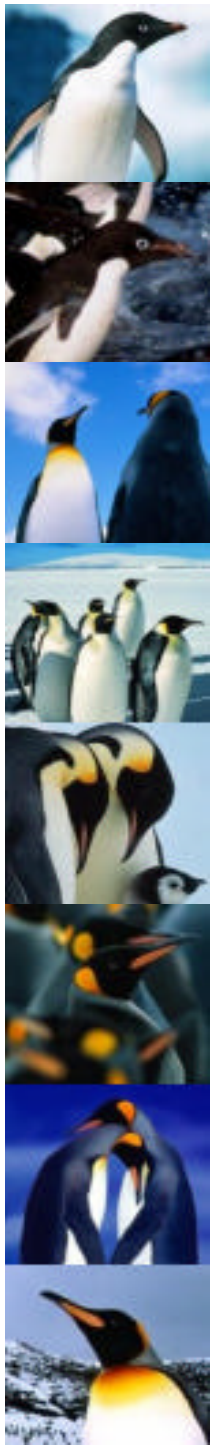


ArticSoft

The challenges

- How do you explain PKI in a way that Managers are able to understand the business requirements and implications without needing to understand more than a marginal amount of technical complexity
- How do you explain what practical alternatives are available
- What would allow managers to make informed judgements

© ArticSoft Ltd 2003

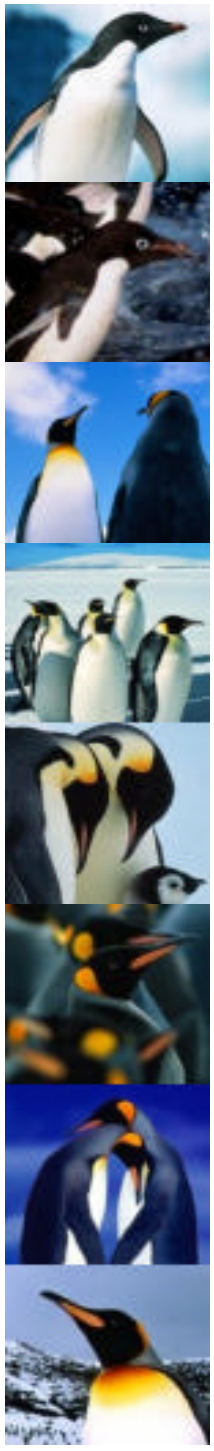


ArticSoft

A potential approach

- Avoid a dissertation on cryptography
- Concentrate on issues that bother management – how do I get my job done – what is the administrative burden – what does this enable me to do more easily – what does this enable me to achieve that I couldn't do before – could I do this more cheaply – what kinds of limitations does this have – before approving a project what should I check on to make sure it doesn't come back and haunt me

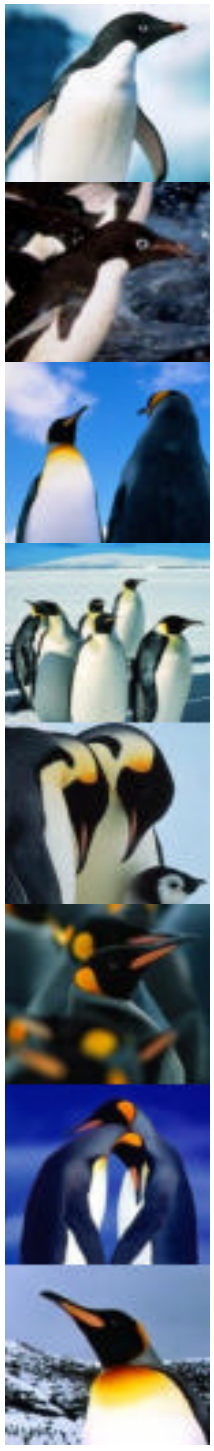
© ArticSoft Ltd 2003



Public key cryptosystems

- PKI is not the only variant in town, but it is the most commonly understood by security practitioners and generally accepted by major suppliers
- The current PKI technology has been developed around the concept of being able to authenticate the identity of entities – people, machines, information
- There is nothing specifically new in the concept of authentication. The issues are about span of control and ability to rely upon information on which you place reliance

© ArticSoft Ltd 2003

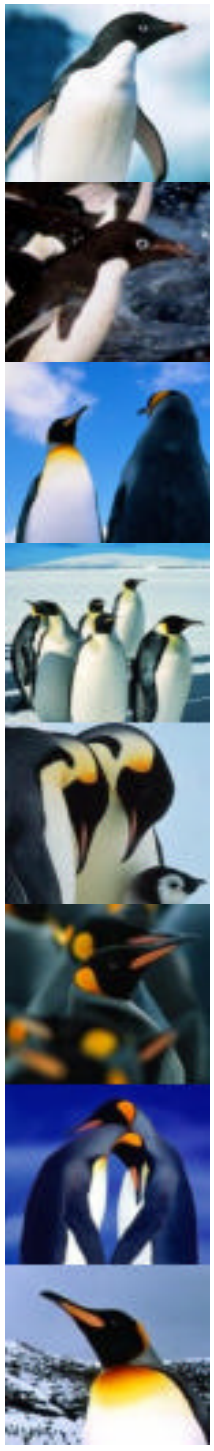


ArticSoft

How can we present ideas?

- In any authentication service there must have been a registration service before authentication can take place
- The critical business feature of authentication is the information that is gained by verifying an entity
- We therefore need to develop scenarios that show authentication, and then develop the argument about what business purpose is being served by it

© ArticSoft Ltd 2003

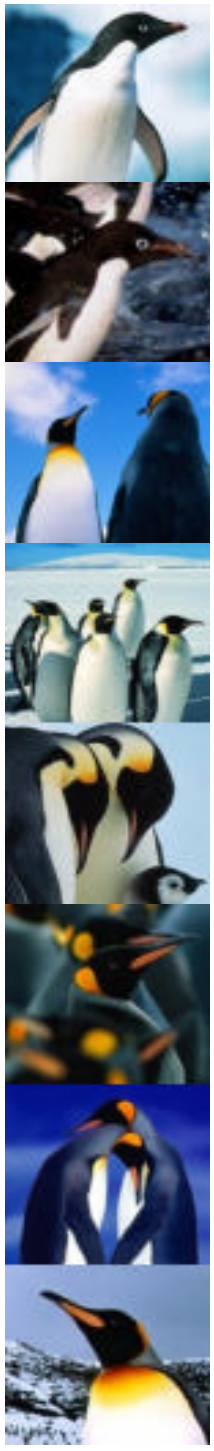


ArticSoft

Our approach

- To describe a number of normal business scenarios
- To describe how these can be facilitated by PKI
- To describe the commonest alternatives
- To describe the registration or processing requirements that must be met to facilitate PKI
- To describe the principal questions that a manager should ask before giving approval

© ArticSoft Ltd 2003



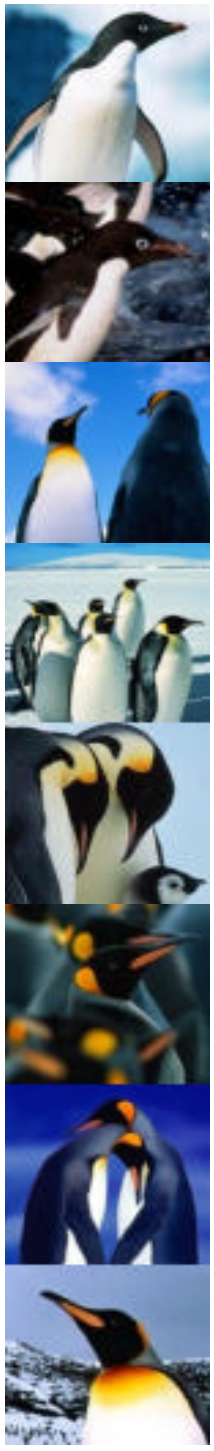
ArticSoft

Introducing the scenarios

Here we are going to break off, and take an initial look at the proposed scenarios that should cover enough ground to be helpful without losing the plot.

We will also look at some preliminary text describing a scenario.

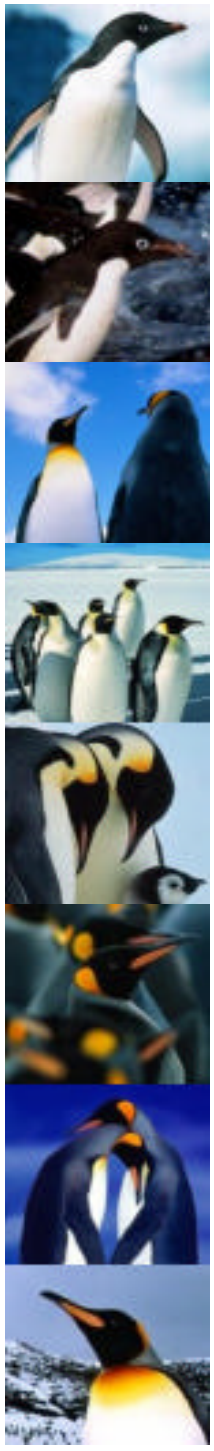
© ArticSoft Ltd 2003



Next steps

- To gain understanding and agreement of the approach, and to receive initial comment(s)
- To canvass inputs on text for the scenarios
- To consider the impact of keeping the guide short enough to be interesting whilst making it long enough to be effective
- To receive any sample text from members and create additional text with a view to moving to the next stage of creating a draft guide

© ArticSoft Ltd 2003



ArticSoft

Questions

Observations

Thoughts

Concerns

Issues

Wisdom

© ArticSoft Ltd 2003