

Rethinking Public Key Infrastructures and Digital Certificates

Rethinking Public Key Infrastructures and Digital Certificates

Building in Privacy

Stefan A. Brands

The MIT Press

Cambridge, Massachusetts

London, England

©2000 Stefan A. Brands

All rights reserved. No part of this book may be reproduced in any form by any electronic or mechanical means (including photocopying, recording, or information storage and retrieval) without permission in writing from the publisher.

Library of Congress Cataloging-in-Publication Data

Brands, Stefan A.

Rethinking public key infrastructures and digital certificates : building in privacy /
Stefan A. Brands.

p. cm.

Includes bibliographical references and index.

ISBN 0-262-02491-8 (alk. hc)

1. Computer networks—Security measures. 2. Computer network protocols. 3.

Data encryption (Computer science). 4. Computer security. I. Title.

TK5105.59 B73 2000

005.8—dc21

00-032866

Dedicated to the memory of Petr Švestka

